

A close-up photograph of a bearded dragon lizard. The lizard is light brown with dark brown, irregular patterns on its body. It has a prominent 'beard' of yellowish skin under its chin. It is resting on a piece of weathered wood, with its front legs visible and its head turned slightly to the right, looking towards the camera. The background is blurred.

# Segurança de Redes de Computadores

# Fundamentos de Segurança de Redes

Compilado por:

Sérgio Simbine

[sergio.simbine@gmail.com](mailto:sergio.simbine@gmail.com)

Março, 2023

## Sérgio Simbine

- ✓ Mestre em Sistemas de Informação pela UEM;
- ✓ Membro do ISACA – *Information Systems Audit and Control Association* (ISACA ID 748519);
- ✓ *Certified Information System Auditor* (CISA) – pela ISACA;
- ✓ *Certified COBIT 5 Foundation* – pela ISACA;
- ✓ *Certified COBIT 4.1* – pela ISACA;
- ✓ *Certified ISO 22301 Lead Auditor* – pela Continuity Link.
- ✓ Consultor de TI: *IT Governance*, Continuidade de Negócios, Gestão de Riscos de TI e Segurança Cibernética
- ✓ Auditor de TI com mais de 20 anos de experiência
- ✓ Docente universitário com mais de 15 anos de experiência

- ✓ Introdução
- ✓ Revisão
- ✓ Conceitos básicos – Redes de Computadores
- ✓ Conceitos básicos – Segurança de Sistemas de Informação
- ✓ Direito Digital
- ✓ Fundamentos de Segurança de Redes
- ✓ Referências bibliográficas

## ✓ Objectivos

➤ Fornecer aos estudantes as habilidades necessárias à investigação de sistemas potencialmente comprometidos em redes corporativas e os principais conceitos e tecnologias fundamentadas em perícia digital ou forense digital para a análise de dispositivos em geral e recuperação de evidências, bem como a elaboração e análise de relatórios periciais.

## ✓ Resultados Esperados (Competências)

- Analisar a volatilidade de evidências e colecta de dados num sistema em execução;
- Recuperar informações parcialmente destruídas;
- Reconstruir a linha temporal dos eventos;
- Prevenir de armadilhas instaladas por invasores;
- Ter a compreensão da lógica dos sistemas de ficheiros

Segundo o CSI (*Computer and Structures, Inc*) e o FBI (*The Federal Bureau of Investigation*), os crimes relacionados com informática e sistema têm vindo a aumentar ao longo dos anos, tal como o têm sido os custos associados aos mesmos.

O termo segurança está, pois, associado a riscos e à prevenção e minimização dos mesmos. Segurança significa a existência de capacidade para se tomarem medidas preventivas que, se não forem suficientemente capazes para evitar as ocorrências indesejadas, maliciosas ou inesperadas, pelo menos prevejam acções a serem tomadas que minimizem as mesmas. O processo de segurança não é algo de que se possa dizer que tem um princípio e um fim bem determinados.

O processo de segurança é constante e continuado ao longo do tempo e implica a não existência de tréguas, pois estas podem constituir-se como vulnerabilidades.

É por isso que a realização de um sistema de segurança tem várias etapas, sendo a primeira uma avaliação do custo/benefício, para que existam garantias de que não se irá efectuar um investimento em segurança de valor superior ao que se pretende tornar seguro, incluindo os custos com pessoal e tendo em conta que o processo necessitará de técnicos a trabalhar a tempo inteiro.

Segurança de rede de computadores é historicamente considerado como um tópico complicado apenas tratado por especialistas bem treinados na matéria.

Entretanto, uma vez que um crescente número de pessoas e empresas são atacadas, daí que é crescente o número de pessoas que se interessam pela segurança de rede.

Assim, esta cadeira (Segurança de Redes de Computadores) pretende destacar os principais problemas relacionados com a segurança, nas suas várias vertentes, desde segurança física até segurança lógica e aplicacional.

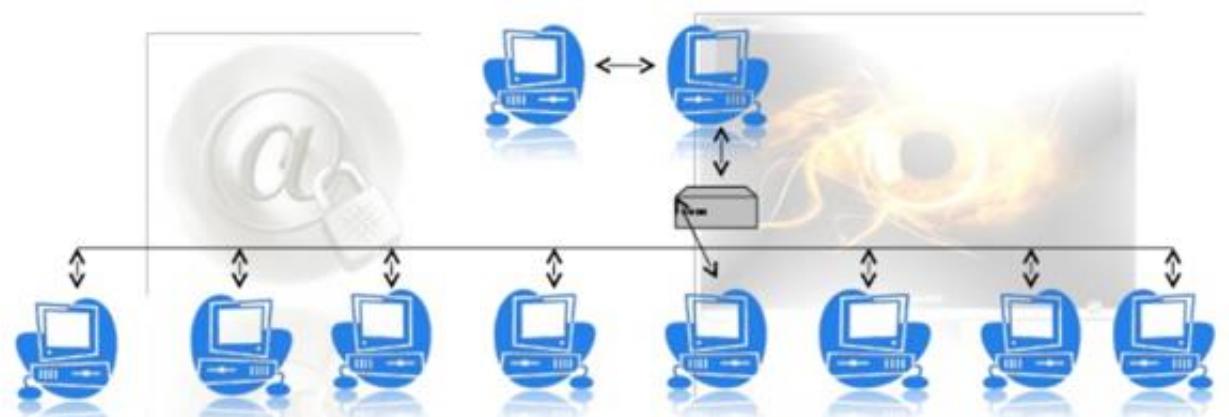
A ameaça é real!

# Revisão - Redes



## O que é Redes de Computadores?

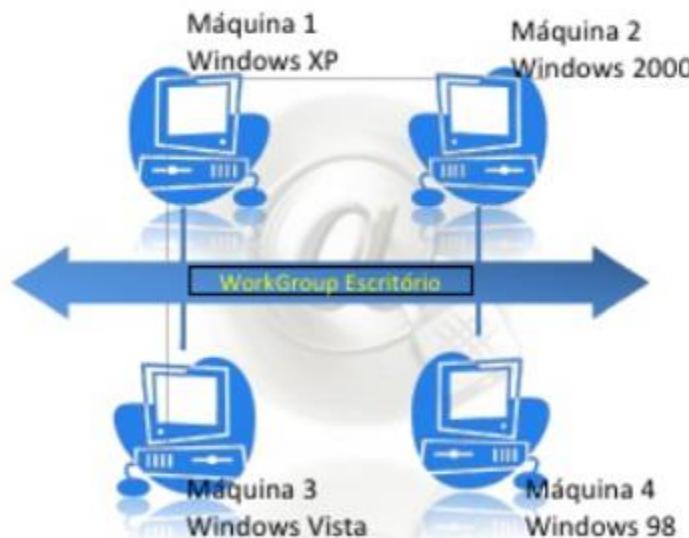
- ✓ É um conjunto de dispositivos (normalmente conhecido como nós) conectados por links de comunicação. Um nó pode ser um computador, uma impressora ou outro dispositivo de envio e/ou recepção de dados, que estejam conectados a outros nós da rede.
- ✓ É a união de 2 ou mais computadores ou outros dispositivos conectados entre si compartilhando serviços e dados.



## Redes de Computadores:

### *Classificação Básica*

#### Ponto a Ponto



#### Baseadas em Servidor



## Redes de Computadores:

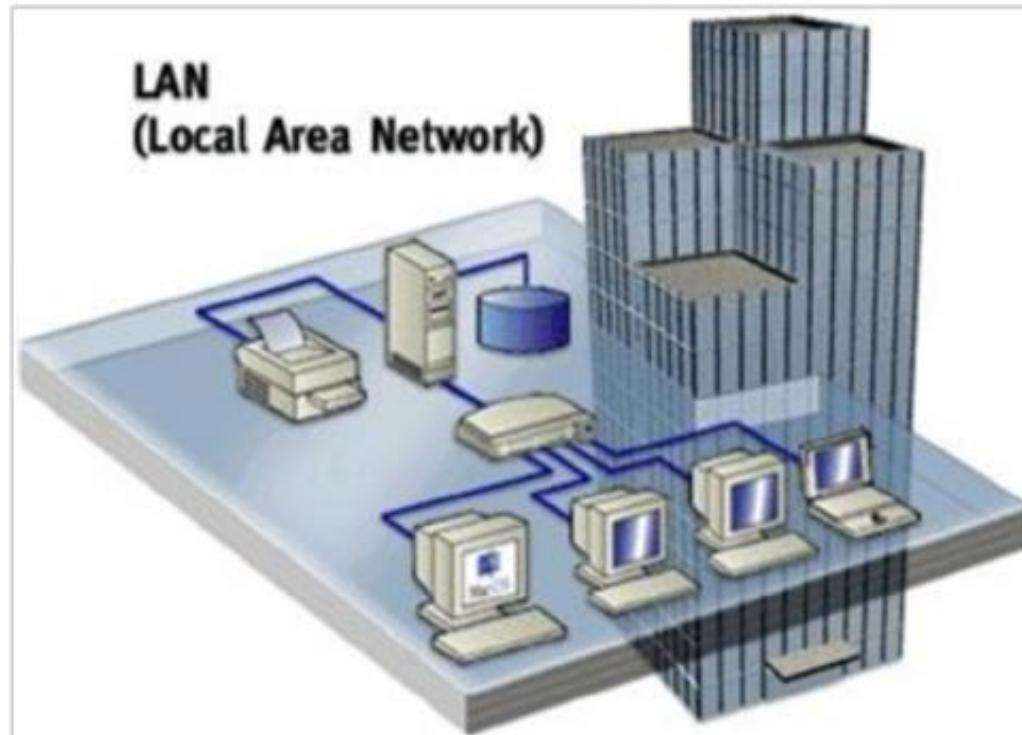
### *Arquitetura – Ethernet*



## Redes de Computadores:

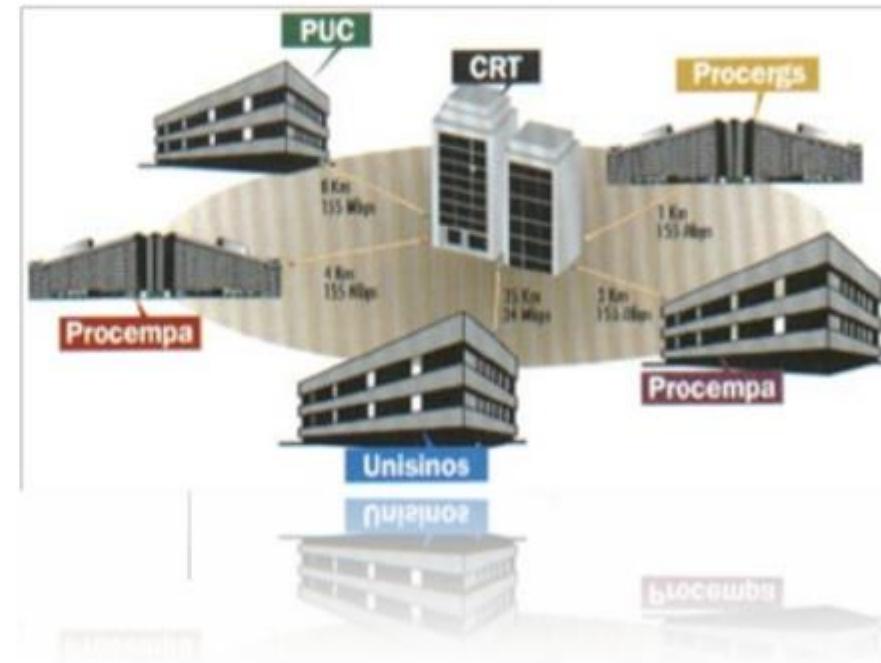
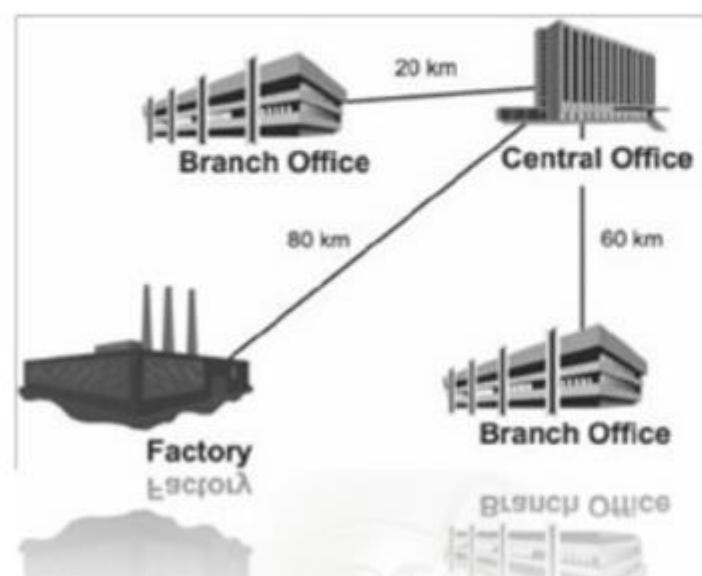
### *Geografia - LAN*

“É uma rede, limitada em uma área geográfica, na qual computadores e outros equipamentos são conectados através de um cabeamento comum”



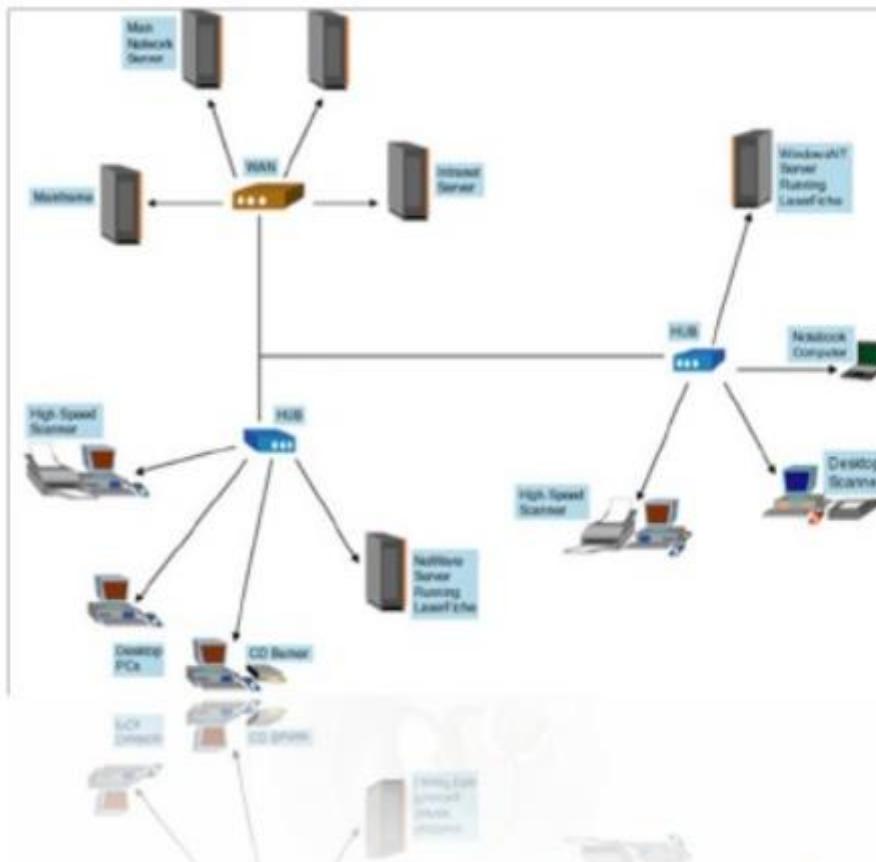
## Redes de Computadores:

### *Geografia - MAN*

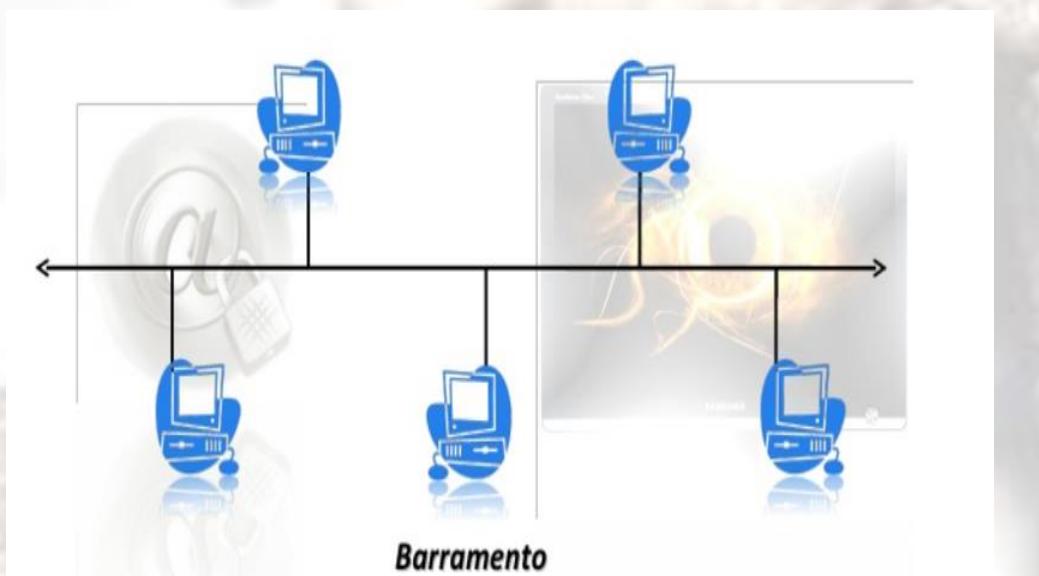
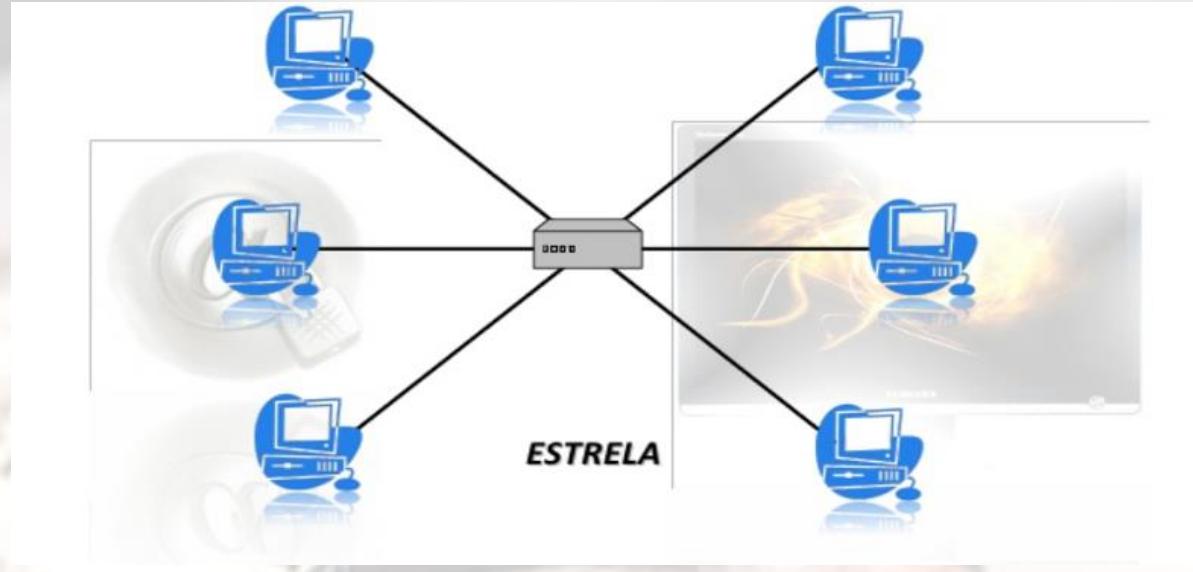
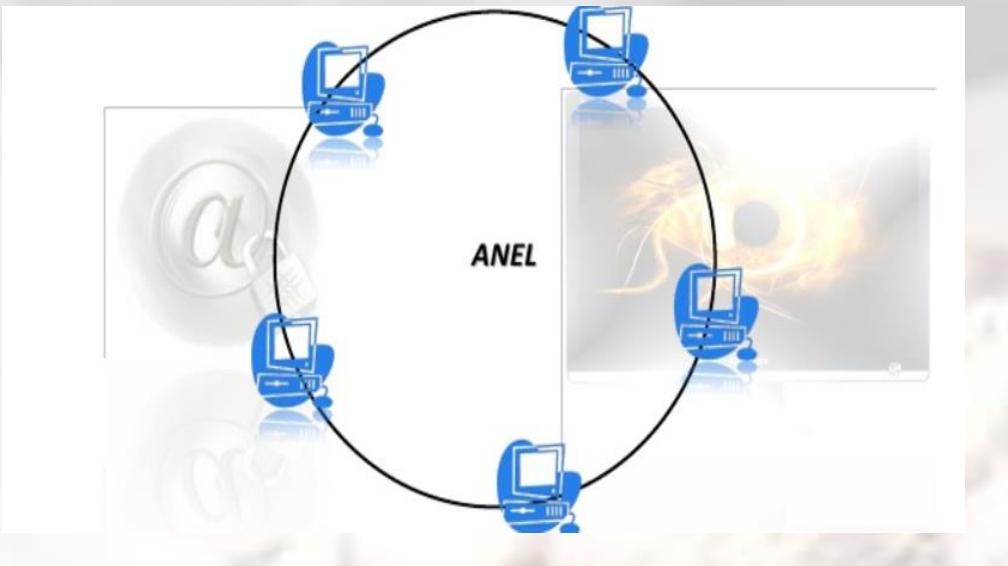


## Redes de Computadores:

### *Geografia - WAN*



## Redes de Computadores: Topologia



## Critérios de Redes:

Uma rede deve ser capaz de atender a certo número de critérios. Os mais importantes são:

- ✓ Desempenho
- ✓ Confiabilidade
- ✓ Segurança

## DESEMPENHO:

- ✓ O desempenho pode ser medido de várias formas, inclusive pelo tempo de trânsito. Tempo de trânsito é a quantidade de tempo necessária para uma mensagem trafegar de um dispositivo a outro. O tempo de resposta é o tempo decorrido entre uma solicitação e sua resposta. Depende do número de utilizadores, tipos de meios de transmissão, capacidades do hardware conectado e eficiência do software.
- ✓ O desempenho é normalmente avaliado por duas métricas de rede: **capacidade de vazão** (*throughput*) e **atraso** (*delay*).
  - Em geral, precisamos de mais capacidade de vazão e menos atraso.
  - Ao mesmo tempo em que podemos aumentar a capacidade de vazão, enviando mais dados, podemos aumentar o delay em razão do congestionamento do tráfego na rede.

- ✓ **CONFIABILIDADE** - Além da precisão na entrega, a confiabilidade das redes é medida pela frequência de falhas, pelo tempo que o link leva para se recuperar de uma falha e pela robustez da rede em caso de uma catástrofe.
- ✓ **SEGURANÇA** - Entre as principais questões de segurança de rede, temos: proteção ao acesso não autorizado de dados, proteção dos dados contra danos e o desenvolvimento e a implementação de políticas e procedimentos para a recuperação de violações e perdas de dados.



## **INTERNET:**

- ✓ A Internet revolucionou diversos aspectos do nosso dia a dia, afectou a forma pela qual os negócios são realizados, bem como a maneira com a qual gastamos nosso tempo de lazer.

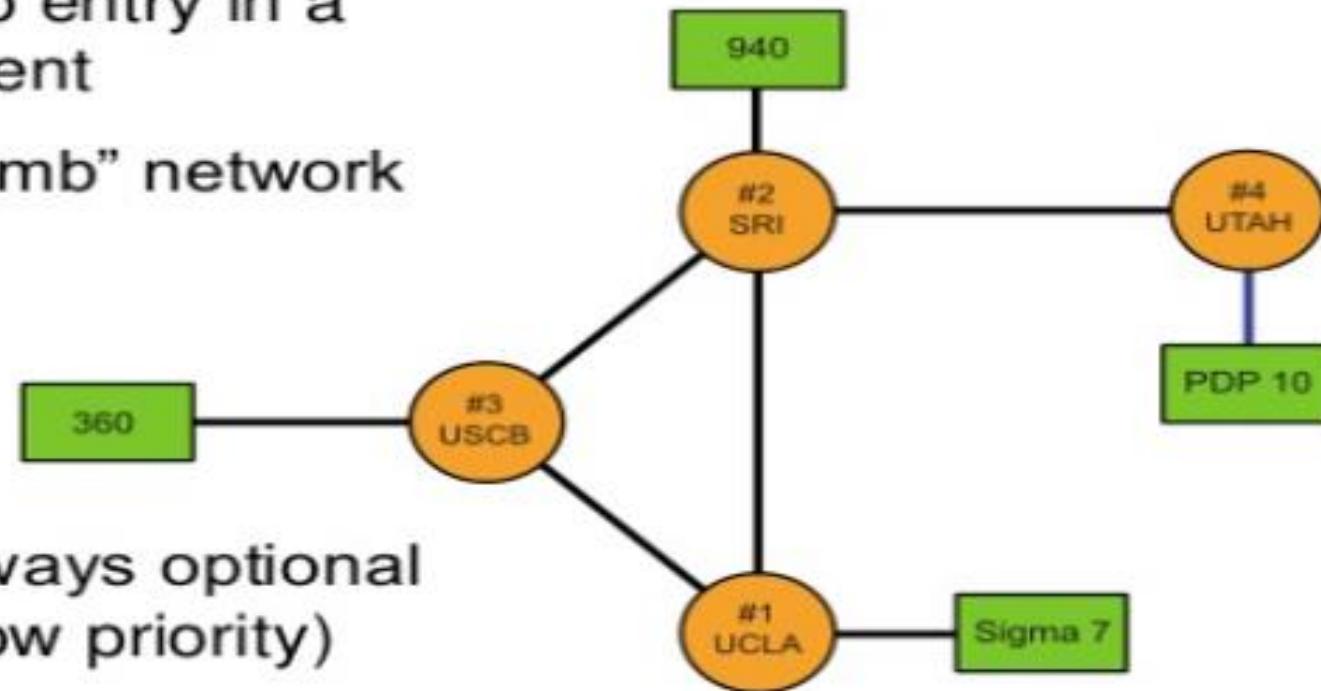


## INTERNET:

- ✓ Inicialmente, grande parte dos acessos à Internet eram realizados por meio de conexão discada com velocidades que dificilmente ultrapassavam 56 Kbps. O usuário, de posse de um modem e de uma linha telefônica, se conectava ao provedor de acesso e mantinha esta conexão apenas pelo tempo necessário para realizar as ações que dependessem da rede.
- ✓ Desde então, grandes avanços ocorreram e novas alternativas surgiram, sendo que actualmente grande parte dos computadores pessoais ficam conectados à rede pelo tempo em que estiverem ligados e a velocidades que podem chegar a até 100 Mbp.

## A internet é Segura?

- The Internet was designed for open connectivity
- For low barriers to entry in a trusting environment
- A deliberately “dumb” network



- “Security” was always optional (and normally a low priority)

## Questões reais!...

- If you ask...
  - “Is the Internet secure?”
  - “Can the Internet be secured?”
  - “Can society ever be safe?”
  - The truthful answer is “**No**”
  
- But if you ask...
  - “Can my services/networks/transactions be secured?”
  - “Can the Internet be used securely?”
  - “Can I stay safe?”
  - The answer is probably “**Yes**” (but with care!)

Você já  
se  
imaginou  
sem  
internet?



**Estamos vivendo uma revolução:**

Não mais procuramos por notícias, produtos ou serviços;

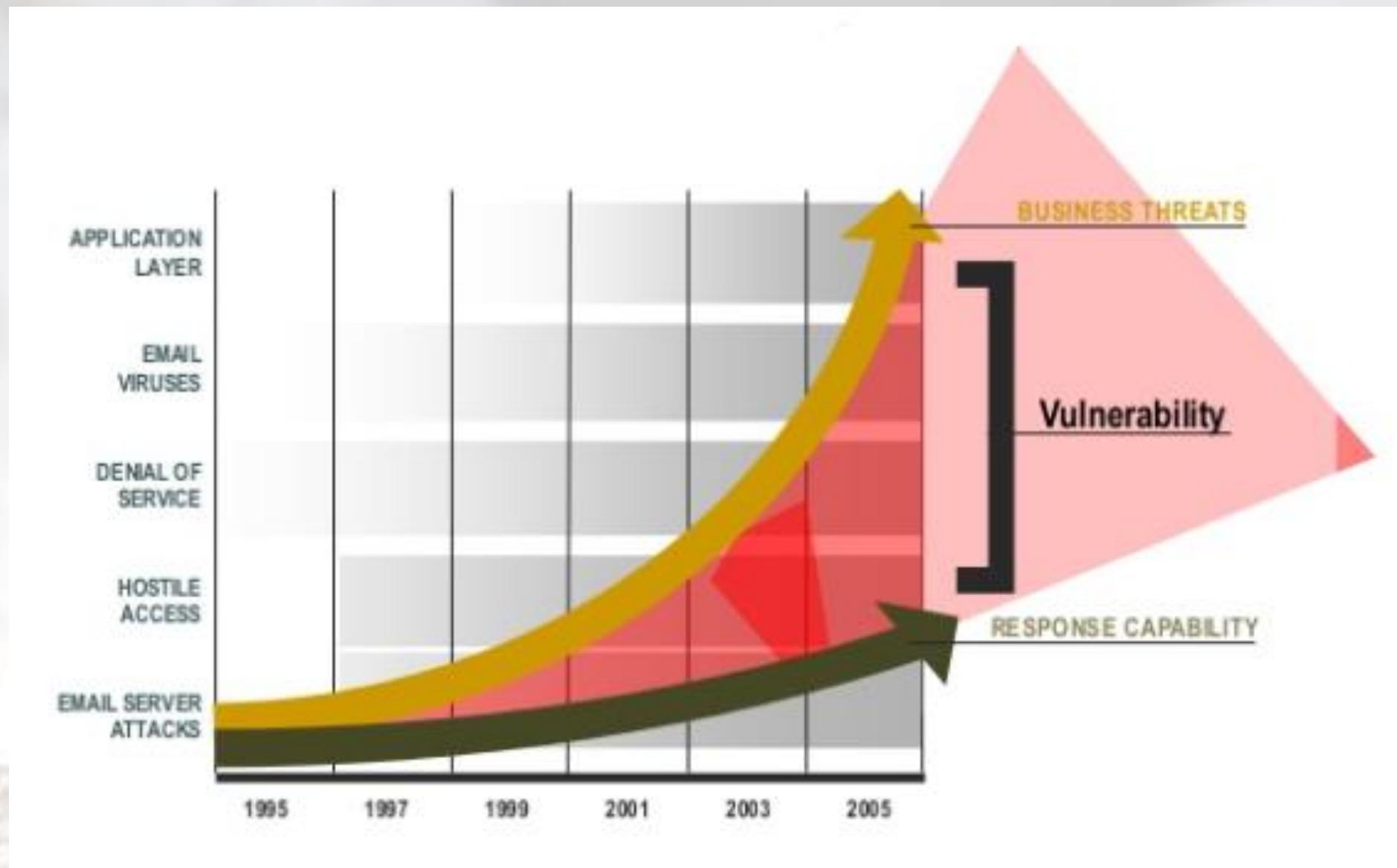
eles nos encontram via mídias sociais,

Mídia social não é um modismo, é uma mudança fundamental  
na maneira como nos comunicamos!

Resultados da pesquisa de segurança FBI-CSI 2020 (cerca de 517 empresas americanas dos mais diversos portes):

- Mais de 50% das empresas destinam menos de 5% do orçamento de TI em segurança;
- Apenas 68% das empresas possuem Política de Segurança da Informação formalizada;
- 52% investem menos de 1% do orçamento de segurança em treinamento dos funcionários;
- 60% das empresas não terceirizam qualquer parte da segurança da informação e os outros 27% terceirizam menos de 20%;

- ✓ Popularização do uso de redes;
  - Intercâmbio de acesso;
  - Mobilidade;
  - Sistemas distribuídos;
- ✓ Redes se tornaram maiores, mais complexas e com maior volume de dados;
- ✓ Os sistemas operacionais são naturalmente inseguros;
  - Até o Linux (que é considerado um dos mais seguros) começa a ser alvo de mais ataques.



Resultados da pesquisa de segurança FBI-CSI 2020 (cerca de 517 empresas americanas dos mais diversos portes):

- Mais de 50% das empresas destinam menos de 5% do orçamento em segurança de TI;
- ✓ 56% das empresas tiveram incidentes de segurança em 2020;
- ✓ Maioria dos prejuízos vem de ataques externos (51% disseram que os incidentes não envolviam funcionários);
- ✓ Tipos de incidentes mais encontrados:
  - Vírus (50%), Roubo de laptop (42%), Abuso de funcionário (44%), DoS (21%)
- ✓ Tecnologias de prevenção/defesa mais usadas:
  - Antivírus (97%), Firewalls (94%), VPN (85%), Anti-spyware (80%), IDS/IPS (69%), filtro de URL (65%).

## ➤ Pesquisas a Nível Nacional?

## ALGUNS ATAQUES NA INTERNET:

- ✓ **Furto de dados:** informações pessoais e outros dados podem ser obtidos tanto pela interceptação de tráfego como pela exploração de possíveis vulnerabilidades existentes em seu computador.
- ✓ **Uso indevido de recursos:** um atacante pode obter o acesso a um computador conectado à rede e utilizá-lo para a prática de actividades maliciosas, como acesso a arquivos, disseminar spam, propagar códigos maliciosos, desferir ataques e esconder a real identidade do atacante.

## TIPOS DE AMEAÇAS NA INTERNET:

- ✓ **Varredura:** um atacante pode fazer varreduras na rede, a fim de descobrir outros computadores e, então, tentar executar ações maliciosas, como ganhar acesso e explorar vulnerabilidades.
- ✓ **Interceptação de tráfego:** um atacante, que venha a ter acesso à rede, pode tentar interceptar o tráfego e, então, colectar dados que estejam sendo transmitidos sem o uso de criptografia.
- ✓ **Exploração de vulnerabilidades:** por meio da exploração de vulnerabilidades, um computador pode ser infectado ou invadido e, sem que o dono saiba, participar de ataques, ter dados indevidamente colectados e ser usado para a propagação de códigos maliciosos.

## TIPOS DE AMEAÇAS NA INTERNET:

- ✓ **Ataque de negação de serviço (DoS):** um atacante pode usar a rede para enviar grande volume de mensagens para um computador, até torná-lo inoperante ou incapaz de se comunicar.
- ✓ **Ataque de força bruta:** computadores conectados à rede e que usem senhas como método de autenticação, estão expostos a ataques de força bruta. Muitos computadores, infelizmente, utilizam, por padrão, senhas de tamanho reduzido e/ou de conhecimento geral dos atacantes.
- ✓ **Ataque de personificação:** um atacante pode introduzir ou substituir um dispositivo de rede para induzir outros a se conectarem a este, ao invés do dispositivo legítimo, permitindo a captura de senhas de acesso e informações que por ele passem a trafegar.

## CUIDADOS GERAIS:

- ✓ **Mantenha seu computador actualizado**, com as versões mais recentes e com todas as actualizações aplicadas;
- ✓ **Utilize e mantenha actualizados mecanismos de segurança**, como programa antimalware e firewall pessoal;
- ✓ **Seja cuidadoso** ao elaborar e ao usar suas senhas;
- ✓ **Utilize conexão segura** sempre que a comunicação envolver dados confidenciais;
- ✓ Caso seu dispositivo permita o **compartilhamento de recursos**, desactive esta **função** e somente a active quando necessário e usando senhas difíceis de serem descobertas.

## CUIDADOS GERAIS:

- ✓ **Mantenha seu computador actualizado**, com as versões mais recentes e com todas as actualizações aplicadas;
- ✓ **Utilize e mantenha actualizados mecanismos de segurança**, como programa antimalware e firewall pessoal;
- ✓ **Seja cuidadoso** ao elaborar e ao usar suas senhas;
- ✓ **Utilize conexão segura** sempre que a comunicação envolver dados confidenciais;
- ✓ Caso seu dispositivo permita o **compartilhamento de recursos**, desactive esta **função** e somente a active quando necessário e usando senhas difíceis de serem descobertas.

## ÉTICA & INTERNET:

- ✓ O comportamento humano on-line costuma ser menos “maduro” do que em ambientes sociais normais
- ✓ A demanda por profissionais de segurança de sistemas está crescendo tão rapidamente
- ✓ O governo dos EUA e o Internet Architecture Board (IAB) definem uma política referente ao uso aceitável da Internet voltada para os cidadãos dos EUA (**E nós que normas temos no nosso país?**)
  - A política não é uma lei ou obrigatória

# Actividade



## **TRABALHO INDIVIDUAL 1:**

1. Leia e faça o resumo (minimo de 2 paginas e maximo 3) dos seguintes documentos:
  - Artigo 1 – *Network security: History, importance and future*
  - Secção 1.1 *Computer security concepts* , do livro *Criptography and Network Security: principles and practice*, William Stallings, 6 Ed
2. Responda as seguintes questões:
  - a) Defina o conceito de Segurança de Redes de Computadores.
  - b) Diga qual é a importância da Segurança de Redes de Computadores
  - c) Descreva os principais desafios relacionados com a segurança de Redes de Computadores

**Data de Entrega: 27/02/2023**

# Revisão – Modelo OSI



## **Modelo OSI:**

Nos primórdios das redes de computadores, existiam alguns problemas;

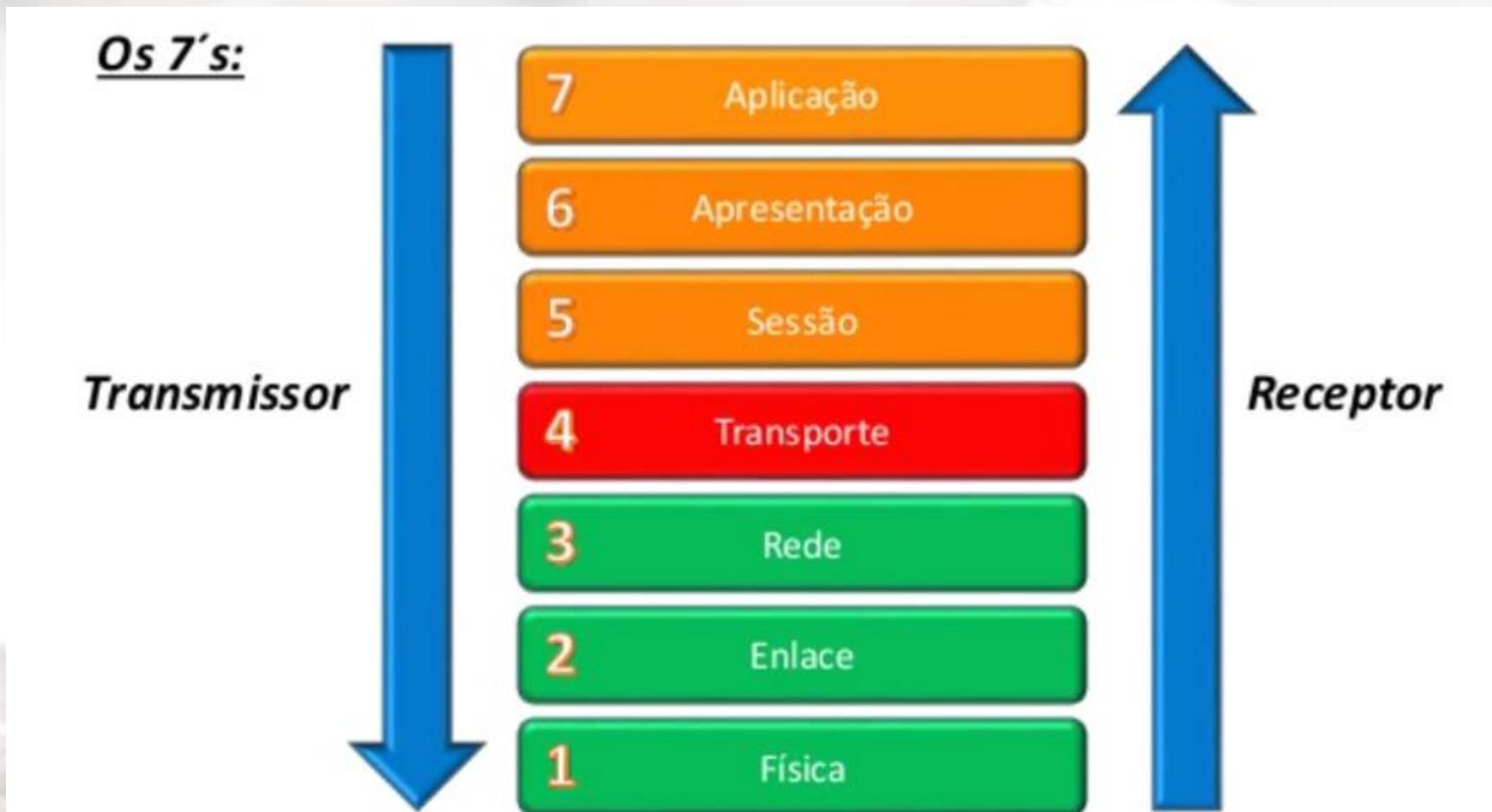
- ✓ Fabricantes criavam sistemas com arquitecturas fechadas;
- ✓ Não existia uma padronização de comunicação entre redes;
- ✓ Comunicar redes de fabricantes diferentes sempre era dificuldade;

Para solucionar o problema , foi criado o padrão **OSI!!!**

## Modelo OSI:

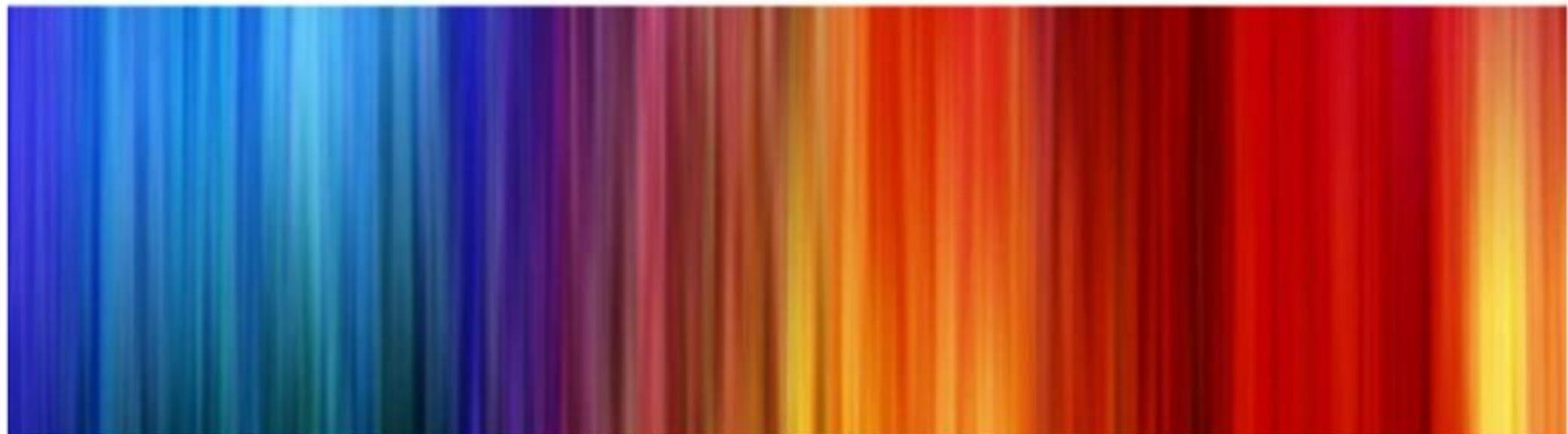
- ✓ É uma padronização;
- ✓ Estabelecido no final de 1970 pela *International Organization for Standardization* (ISO);
- ✓ Tem como principal funcionalidade cobrir todos os aspectos das comunicações de dados em redes;
- ✓ É um sistema aberto e tem como objectivo efectuar a comunicação entre dois sistemas diferentes;
- ✓ Estabelece uma padronização sem realizar mudanças em hardware ou no software;
- ✓ Possui camadas ;
- ✓ Todas as camadas se relacionam entre si;
- ✓ OSI não é um protocolo é modelo para projectar uma arquitectura de rede.

## Camadas do modelo OSI:



## Camadas do modelo OSI:

- Composta por 7 camadas.
- Representam a forma de como os dados devem ser percorridos dentro de uma rede.
- Cada camada requisita os serviços da camada inferior relacionada a ela.



## Camadas de Suporte à Rede:



## Camada Física:

- ✓ Tem como principal objectivo coordenar as funções necessárias para transportar o fluxo de bits dentro de um meio físico;
- ✓ Define as características da interface entre dispositivos e o meio de transmissão;
- ✓ Nesta camada trabalham com o bit “bruto”;
- ✓ Não existe nenhuma interpretação dos bits nesta camada;
- ✓ Nesta camada os bits são transmitidos e codificados em sinais eléctricos, ópticos ou de acordo com o meio físico representado;

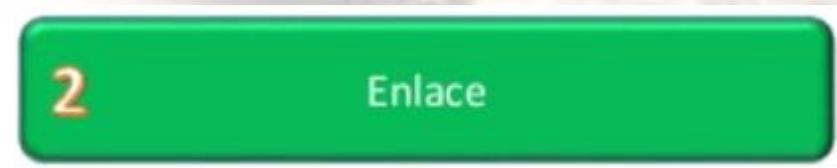
**Dispositivos:** Cabos de cobre, fibra óptica, repetidores, interfaces seriais.



## **Camada de Elance:**

- ✓ Comunica-se com a camada física e tem como objectivo transformar os dados brutos em dados confiáveis para o envio e recebimento;
- ✓ Nesta camada os bits são divididos em unidades de dados chamados de frames;
- ✓ Inclui o endereço físico do emissor e do receptor no pacote. Em uma rede um pacote específico pode passar por mais de um computador até chegar ao destino;
- ✓ Identifica possíveis erros nos pacotes e retransmite frames danificados ou perdidos;

**Dispositivos:** Switches, placas de rede

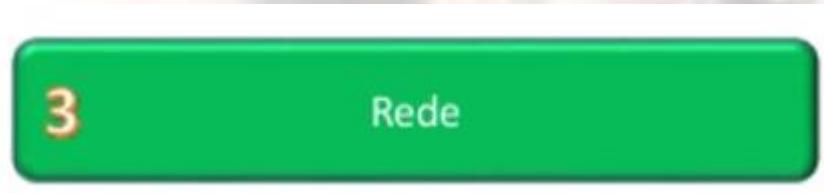


## **Camada de Rede:**

- ✓ Tem como finalidade efectuar a entrega de um pacote desde a sua origem até o seu destino;
- ✓ Trabalha para que a entrega de pacotes aconteça em redes diferentes;
- ✓ Caso dois sistemas estejam na mesma rede; não existe a necessidade desta camada.

**Dispositivos:** Roteadores , Switches.

**Protocolos:** IP.



## Camadas de Ligação:



## **Camada de Transporte:**

- ✓ Comunica-se as camadas de rede e de sessão;
- ✓ Tem como principal funcionalidade garantir que os pacotes sejam montados correctamente, formando uma mensagem;
- ✓ Controla o fluxo de erro de uma mensagem garantindo sua integridade ;
- ✓ É a ligação entre meio físico e o meio lógico.

**Protocolos:** TCP, UDP.



## Camadas de Suporte ao Utilizador:



## Camada de Sessão:

- ✓ Comunica-se as camadas de rede e de sessão;
- ✓ Cria Checkpoints, pontos de verificação ou pontos de sincronização;
- ✓ Garante a comunicação entre dois sistemas mantendo um diálogo;
- ✓ Caso ocorra falha na comunicação, o mesmo dado não é enviado para receptor ou para o emissor;
- ✓ Por exemplo:
  - Caso seja enviado um arquivo com 100 páginas, existem checkpoints a cada 10 páginas garantindo o que foi enviado e recebido.

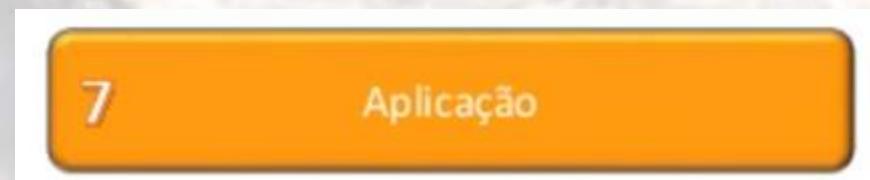


## Camada de Apresentação:

- ✓ Nesta etapa pode acontecer a criptografia das informações;
- ✓ A criptografia garante que as informações serão enviadas de forma segura e confidencial;
- ✓ Pode-se comprimir os dados reduzindo o número de bits enviados;
- ✓ A compressão é muito importante em sites webs, conteúdos multimídias, como áudio, vídeo e músicas;
- ✓ Executa-se também nesta etapa a tradução das informações de acordo com o sistema de codificação de cada sistema ou aplicação,

## Camada de Aplicação:

- ✓ Nesta etapa pode acontecer a criptografia das informações;
- ✓ Camada onde os utilizadores acedem os software utilizados dentro de uma rede de computadores;
- ✓ Nesta camada normalmente encontra-se os seguintes software de rede:
  - Navegadores;
  - Terminal de Rede Remoto;
  - Transferência de arquivos;
  - Correios electrónicos,
  - Serviços de directórios.



## Em Resumo:

- ✓ Modelo OSI tem como finalidade criar uma padronização em redes de computadores;
- ✓ Foi padronizado pela ISO;
- ✓ Tornou-se um padrão aberto;
- ✓ Possui 7 Camadas;
- ✓ Cada camada se comunica entre si;
- ✓ As camadas ajudam a isolar problemas de redes dentro de suas camadas.



# Actividade



## **TRABALHO INDIVIDUAL 2:**

1. Leia e faça o resumo dos seguintes artigos: Artigo 2 – Ataques na camada do Modelo OSI e Arigo 3 - Man in the middle (mitm) attack :
2. Descreva os seguintes ataques.
  - a) IP Address Spoofing
  - b) Routing attacks
  - c) SSL Hijacking
  - d) Program Logic Flaws
3. Para cada um dos ataques descritos na pergunta anterior (pergunta 2), diga quais são as medidas de mitigação recomendadas para cada um deles.
4. Na sua opinião/experiência, diga:
  - a) Diga qual é o ataque mais comum que se verifica em Moçambique. Justifique a sua resposta.
  - b) Na sua opnião, diga qual das camadas do Modelo OSI é mais vulnerável a ataques. Porquê?

**Data de Entrega: 06/03/2023**

# Revisão – Segurança

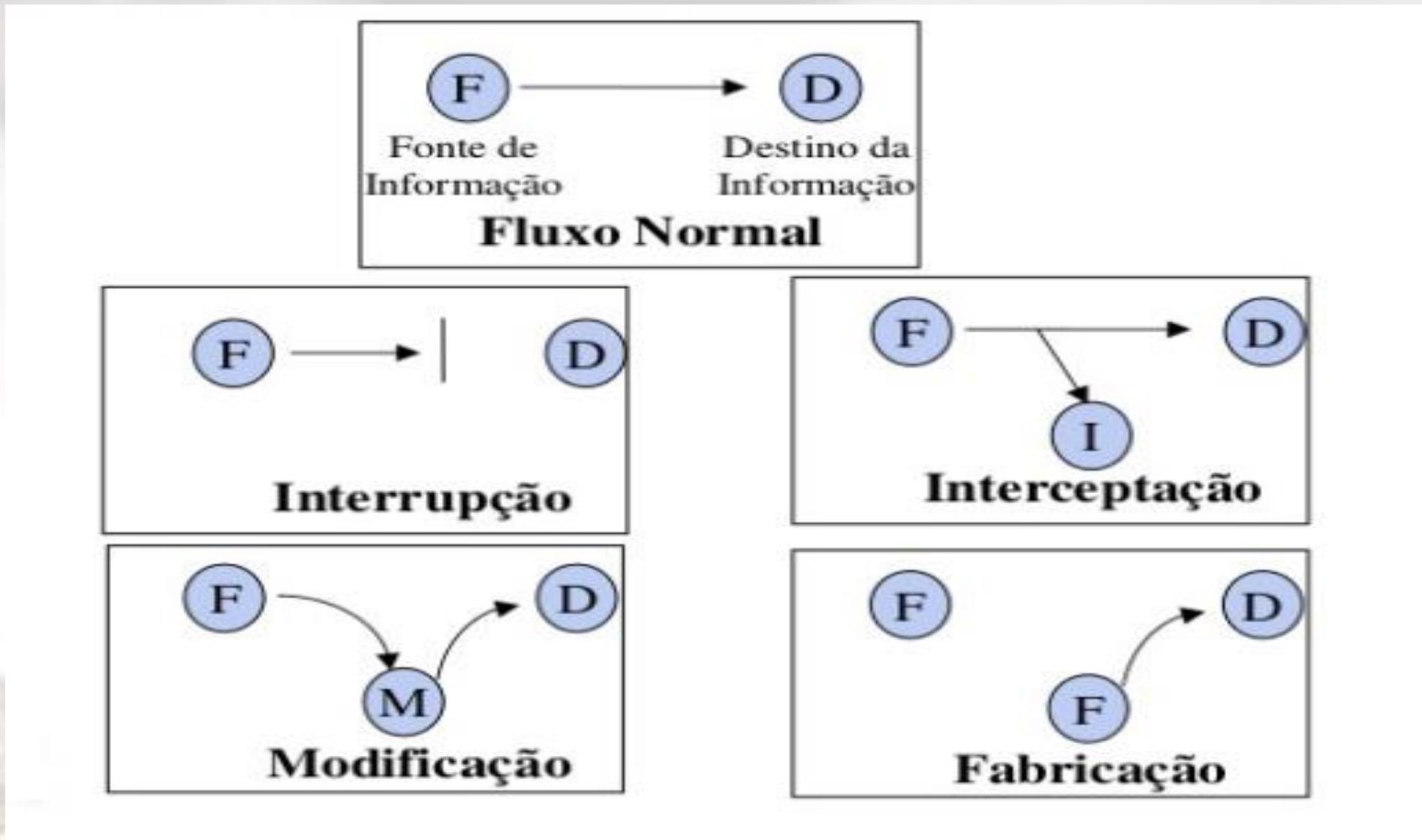


# Revisão – Segurança

## **Segurança:**

- ✓ **Autenticação** – Validade identidade do utilizador;
- ✓ **Controlo de acesso** - Nível de autorizações;
- ✓ **Não-repúdio** – Impedir que seja negada a autoria ou a ocorrência de um envio ou recepção de informação;
- ✓ **Confidencialidade** – Tem a ver com a divulgação (*closure*) não autorizada;
- ✓ **Integridade** – Alteração não autorizada na informação;
- ✓ **Disponibilidade** – Acesso à informação.
- ✓ **Vulnerabilidade:**
  - Ponto fraco inerente à natureza do sistema;
  - Brecha; ponto fraco ou falho que pode ser explorado.
- ✓ **Ameaça** – Algo que afecte o funcionamento da rede, comprometendo sua operação, disponibilidade ou integridade;
- ✓ **Ataque** – Modo utilizado para explorar determinada vulnerabilidade;
- ✓ **Contra-medidas** – Métodos de defesa dos ataques.

## Ameaças à Segurança:



## Ameaças à Segurança:

- ✓ **Interruption (Interrupção)** - é uma ameaça à **Disponibilidade (Availability)**
- ✓ **Interception (Interceptação)** - é uma ameaça à **Confiencialidade (Confidentiality)**
- ✓ **Modification (Modificação)** - é uma ameaça à **Integridade (Integrity)**
- ✓ **Fabrication (Fabricação)** - é uma ameaça à **Autenticidade (Authenticity)**



## **Segurança Física:**

✓ Para proteger a informação, a preocupação deve começar no próprio ambiente físico que compõe a instalação onde a informação se localiza.

- Segurança da sala de equipamentos;
- Segurança dos equipamentos;
- Redundância;
- Segurança no fornecimento de energia;
- Savaguarda (backup);
- Descarte da informação;

## **Segurança Física:**

### ✓ Segurança de Equipamentos

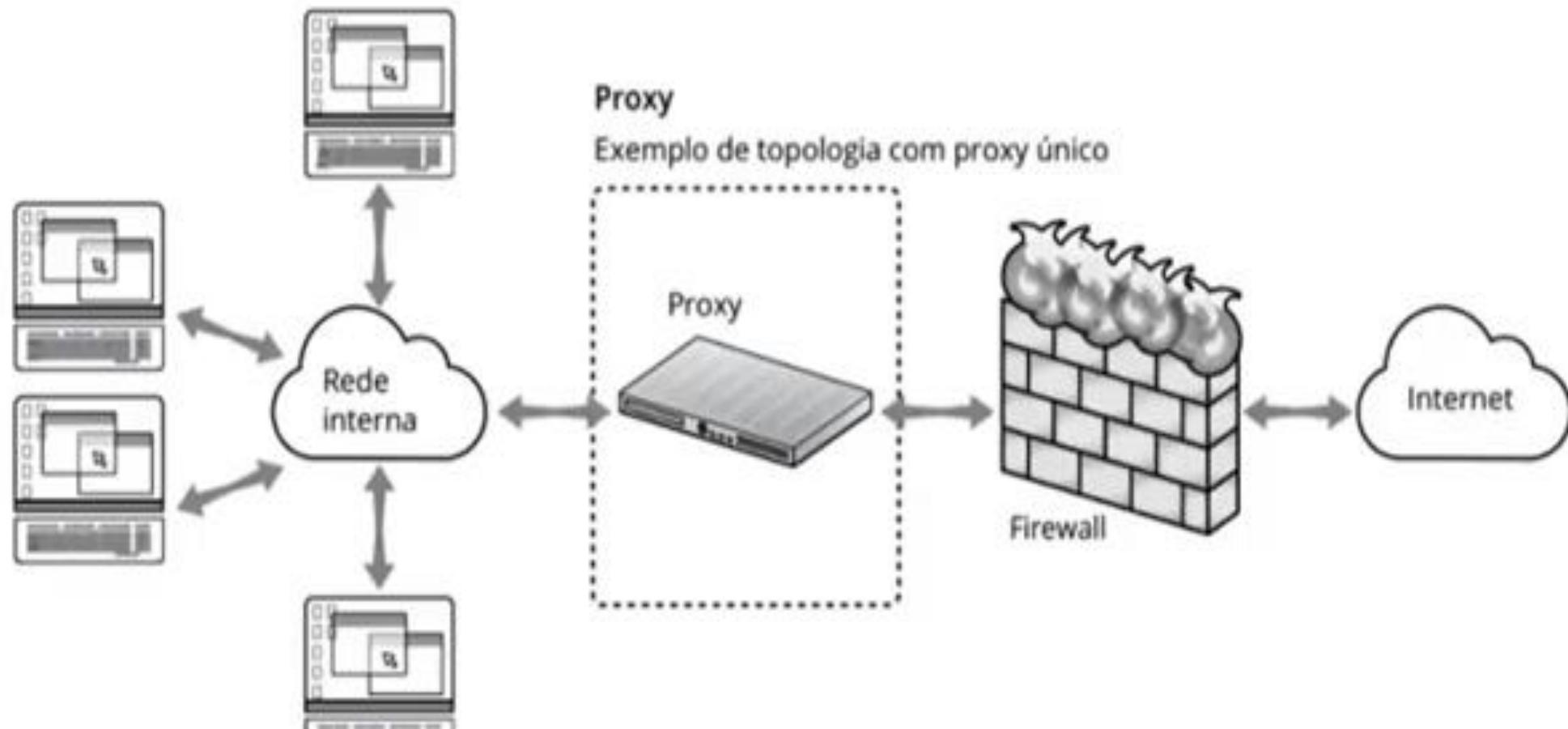
- Instalação e proteção de equipamentos;
- Fornecimento de energia;
- Segurança de cabeamento;
- Manutenção de equipamentos;
- Reutilização alienação segura de equipamentos;
- Segurança de equipamentos fora das instalações.

## **Segurança Física:**

### ✓ Redundância

- O problema mais comum de Segurança é a falha de hardware;
- O mecanismo mais importante para tolerar falhas é a redundância;
- A redundância cria alta disponibilidade, mantendo o funcionamento em caso de falhas de componentes ou sobrecargas;
- Redundância de interface de rede;
- Redundância de CPU's;
- Redundância de discos (RAID);
- Redundância de fontes de alimentação interna;
- Redundância de servidores, etc.

## Segurança Lógica:



## Segurança Lógica:

### ✓ Vírus

- Perda de desempenho (nos dispositivos, intranet e internet);
- Exclusão de arquivos e alteração de dados;
- Acesso a informações confidenciais por pessoas não autorizadas;
- Desconfiguração do Sistema Operacional ;
- Acionamento e desligamento de periféricos.

## Segurança Lógica:

### ✓ Vírus

- Perda de desempenho (nos dispositivos, intranet e internet);
- Exclusão de arquivos e alteração de dados;
- Acesso a informações confidenciais por pessoas não autorizadas;
- Desconfiguração do Sistema Operacional ;
- Acionamento e desligamento de periféricos.

## Principais Ameaças à Segurança:

Método	Definição
<b>Engenharia Social</b>	Técnica usada na obtenção de informações confidenciais, através da exploração do conhecimento ou confiança das pessoas.
<b>Man-in-the-middle</b>	Forma de ataque, em que é interceptada e retransmitida informação trocada entre duas partes num dado canal.
<b>Man-in-the-browser</b>	Consiste na infeção (normalmente, um trojan) do computador da vítima e que é capaz de modificar as comunicações entre o cliente e o servidor de uma maneira imperceptível, quer para a vítima quer para a aplicação.
<b>Trojan</b>	Programa malicioso introduzido num computador sem que a vítima saiba, com o objectivo de abrir uma ligação com o computador do invasor e, assim, este ter total controlo do computador da vítima.
<b>Worms</b>	Programa idêntico a um vírus com a capacidade de replicar-se num sistema inteiro. O objectivo pode ser, por exemplo, sabotar um sistema informático até apagar todos os dados contidos nele.

# Revisão – Segurança

## Principais Ameaças à Segurança:

Método	Definição
<b>Virus</b>	Pedaço de software malicioso com a finalidade de infetar um computador e que este se espalhe por outros computadores.
<b>Phishing</b>	Técnica que tenta obter dados pessoais, através do envio de e-mails fraudulentos que tentam fazer passar-se por uma pessoa ou empresa de confiança e, deste modo, enganar a vítima.
<b>Keylogger</b>	Programa capaz de capturar todas as teclas marcadas pelo utilizador.
<b>Spyware</b>	Programa de computador que é instalado no computador da vítima e tem a capacidade de recolher informações sobre a mesma e depois envia esses dados para outra entidade.
<b>Ransomware</b>	Tipo de malware que restringe o acesso ao computador ou aos arquivos, exibindo uma mensagem em que exige um pagamento para remover a restrição, por exemplo, através de e-mails com anexos maliciosos ou websites infectados

# Revisão – Segurança

## Principais Ameaças à Segurança:

Método	Definição
<b>Botnet</b>	Conjunto de computadores infectados que são controlados remotamente, funcionando, por exemplo, como um exército de computadores que realizam diversas tarefas como enviar e-mails com spam, propagação de malware.
<b>Clickjacking</b>	Método que utiliza as acções de um utilizador numa determinada página web para realizar operações maliciosas. O atacante coloca um iframe num elemento clicável, por exemplo, um botão, de forma a conseguir que a vítima clique nesse iframe e o invasor, sem o conhecimento da vítima, realize uma operação por si definida.
<b>Negação de Serviço</b>	É um ataque que consiste em fazer diversas tentativas ao computador/serviço alvo (ex. servidor web) para que tenham dificuldade ou mesmo sejam impedidos de executar suas tarefas, por outras palavras, sobrecarregam os sistemas. Uma variante deste ataque, muito utilizado, é o DDoS (Negação de Serviço Distribuído): é um ataque em rede, em que um computador mestre controla um certo número de computadores cliente para inundar o alvo com tráfego, através da utilização de um software específico para o efeito.
<b>SQL Injection</b>	Isso acontece quando o invasor insere código malicioso em um servidor que usa o Structured Query Language. As SQL Injections só são bem-sucedidas quando existe vulnerabilidade de segurança. Nesse caso, o ataque forçará o servidor a fornecer acesso ou modificar dados.

# Direito Digital



## Mas por que isso me interessa?

- ✓ Porque isso pode afectar a sua vida directamente.
- ✓ Seu e-mail é o seu endereço electrónico, similar ao seu endereço residencial (Rua..., número...)
- ✓ Seu computador (ou dispositivo) é a porta de entrada para a sua privacidade... para a sua casa.
- ✓ Sob a óptica do Direito Digital, como no mundo virtual não existem fronteiras, é preciso compreender como funcionarão as leis

## Mas por que isso me interessa?

O Direito Digital enfrenta , dentre outras, as seguintes problemáticas:

- ✓ A ausência de leis aplicáveis;
- ✓ Regulamentação para a guarda apropriada de provas; e
- ✓ Alcanse das leis (princípio da Territorialidade);

- A Testemunha é a máquina



## Uma nova disciplina...

- Informática jurídica e Direito da tecnologia da Informação;
- A propriedade intelectual nas novas mídias;
- Documentos electrónicos, prova electronica e Certificado digital;
- Perícia Digital;
- Crimes Electrónicos;
- Fraude electronica;
- Ética e Educação Digital;
- Responsabilidade Civil e dano moral no Direito Digital;
- Comércio Electrónico;
- Processo Electrónico;



## Crime X Crime digital X Cibercrime

- ✓ É apenas uma questão de nomenclatura.
- ✓ Conceito formal: “Crime é uma conduta (acção ou omissão) contrária ao Direito, a que a lei atribui uma pena
- ✓ Vale ressalvar que o Crime não exclui a Responsabilidade Civil;
- ✓ Não há crime sem lei anterior que o defina. Não há pena sem previa comunicação legal.

## Crime X Crime digital X Cibercrime

O Crime, chamado Digital, pode ser cometido de 2 formas:

- ✓ O Computador como **ferramenta** de apoio ao crime;
- ✓ O Computador como **meio** de realização do crime.

## Algumas Questões de Discussão (**em Grupo 10 minutos**)

- ✓ Caso eu não possua firewall e nem antivirus e seja invadido, o crime será cometido ou não? Fundamente?
- ✓ Da mesma forma se meu smarphone não possuir uma senha de protecção e ser invadido, será crime?
- ✓ Caso a invasão tenha sido executadas por algum estrangeiro que se localize fora das linhas territorias. É ou não é crime?

## Cibercultura

A Cibercultura possui três “leis” fundadoras:

- ✓ A liberação do pólo da emissão;

Pode tudo na Internet / Tem de tudo na Internet

- ✓ O Príncípio de conexão em rede

A rede está em todos os lugares / O verdadeiro computador é a rede / sai “PC” e entra “CC”

- ✓ A reconfiguração de formatos midiáticos e práticas sociais;

Tudo muda ....mas nem tanto

## Cibercultura

A Cibercultura enseja vários fenómenos:

- ✓ Negação do copyright, reconfigurando-o na “remixagem”;
- ✓ Criação da chamada arte electronica;
- ✓ Reinvenção das manifestações e expressões comunicacionais habituais, com ferramentas como os blogs e os podcasts
- ✓ Reconstrução do conceito de “compartilhamento” (redes P2P) e do sentido de “colaboração” (wiki);

## Era da informação

- ✓ Vem após a “era industrial” e é marcada por invenções como microprocessador, a rede de computadores, a fibra óptica e o computador pessoal;
- ✓ Fulcra-se nos conhecimentos científicos, na mão-de-obra qualificada e nas inovações tecnológicas;

## Era da informação

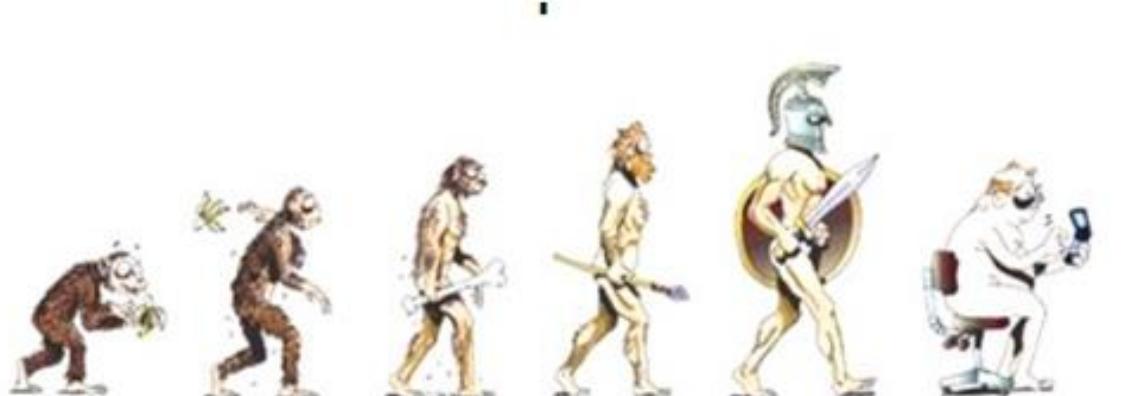
- ✓ Dela surge o conceito de “capital intelectual”(soma do conhecimento de todos em uma organização, proporcionando uma vantagem competitiva), como forma de evidenciar e potencializar a força dos recursos intangíveis;
- ✓ No mesmo berço, surge a **Sociedade da Informação**, também chamada de Nova Economia.

## Assim...

- ✓ Sociedade da Informação = hardware = ênfase e relevância das TICs;
- ✓ Sociedade do Conhecimento = software = conteúdo + significado + conhecimento
  - É caracterizada pelo facto das fontes fundamentais de riqueza serem o conhecimento e os relacionamentos – e não mais o capital, os recursos naturais ou a mão-de-obra.

E...

- ✓ O Direito Digital deve ser visto como um resultado imediato dessa nova sociedade
- ✓ Ao Direito Digital, como a qualquer outro ramo jurídico, é dado um conjunto de princípios gerais e específicos.



## Princípios do Direito Digital

### ✓ Princípios ...

- Verdades fundantes de um Sistema de conhecimento, como tais admitidas, por serem evidentes ou por terem sido comprovadas, mas também por motivos de ordem prática de carácter operacional, isto é, como pressupostos exigidos pela necessidade de pesquisa e praxis.

## Princípios do Direito Digital

### ✓ Princípios Gerais ...

- Princípio da Intervenção Mínima do Estado – que força a acção do Estado de forma fragmentária e subsidiária na protecção dos bens jurídicos a serem tutelados no ambiente virtual;
- Princípio da Privacidade da Informação ou da Autodeterminação Informativa – que visa garantir a pessoa decidir quando e como está disposta a permitir que seja divulgada a sua informação ou a difundí-la por vontade própria.

## Princípios do Direito Digital

### ✓ Princípios Gerais ...

- Princípio da Publicidade – que se refere ao dever atribuído à Administração de dar total transparência a todos os actos que praticar e impõe o fornecimento de todas as informações solicitadas pelos particulares, sejam públicas ou de interesse pessoal, que constem de bancos de dados públicos, já que nenhum acto administrativo pode ser sigiloso;

## Princípios do Direito Digital

### ✓ Princípios Específicos ...

- Princípio da Disponibilidade Universal da Informação – relacionado com a democratização da informação e da inclusão digital, se refere à disponibilidade de informações como bem público sobre qualquer assunto que não viole o direito à intimidade e à propriedade intelectual e não comprometa a segurança pública interna e externa, já que limita a intervenção de outras pessoas e de poderes públicos na vida privada
- Princípio da Justiça Distributiva – base para a evolução da tecnologia e da própria internet, justifica-se para permitir o contínuo desenvolvimento das tecnologias da informação , referindo-se às suas distribuições justas, equitativas e apropriadas à sociedade.

## Princípios do Direito Digital

### ✓ Princípios Específicos ...

- Princípio da Celeridade Normativa – a partir do qual o Estado deve criar institutos jurídicos hagéis (leis, decretos, portarias, actos normativos, etc...) que atendam rapidamente às necessidades sociais na área.
- Princípio da Autorregulamentação – como meio para minimizar a morosidade legal em acompanhar as transformações sociais e tecnológicas experimentadas pela era digital;

## Princípios do Direito Digital

### ✓ Princípios Específicos ...

- Princípio de Autenticidade – em que se deve primar pela garantia de identidade dos utilizadores de informações diante de instrumentos tecnológicos.
- Princípio da Confidencialidade – que diz respeito à disponibilidade da informação apenas para aqueles devidamente autorizados, devendo os agentes emissores proteger a informação.

## Princípios do Direito Digital

### ✓ Princípios Específicos ...

- Princípio da Integração Internacional – para o qual as fronteiras territoriais devem desaparecer , qual reflexo nas relações entre as pessoas, já que a interação entre pessoas de etnias diversas diminui as diferenças, com reflex maior ainda na área commercial, evidenciando a necessidade da formação de blocos económicos para que sectores do mercado possam sobreviver em uma economia globalizada.

## Princípios do Direito Digital

### ✓ Princípios Específicos ...

- Princípio da Cooperação Internacional – Segundo o qual se reconhece a carência de elaboração, aplicação e fiscalização de normas técnicas e jurídicas integradas para permitir uma regulamentação efectiva no ciberespaço.
- Princípio da Separação de Meio e Mensagem – em que se destaca que a mensagem passa a ter valor próprio, deixando de ser valorada pelo meio físico ao qual está vinculada.

## Princípios do Direito Digital

### ✓ Princípios Específicos ...

- Princípio do Domínio Público Internacional – entendido como o conjunto dos espaços cujo uso interessa à sociedade internacional como um todo, mesmo que, em certos casos , tais espaços estejam sujeitos à soberania de uma Nação , tal qual são disciplinados pelo Direito Internacional, de entre outros o mar (e suas subdivisões legais), o espaço aéreo, ...
- Princípio da Identidade Reflexa – que prescreve que tudo o que se encontra no ambiente virtual ése destaca que a mensagem passa a ter valor próum “espelho”da existência no mundo real ou físico, com premissa na permissão de regulamentação de identidade no ciberespaço, seja ela de pessoas físicas ou jurídicas, ciber-cidades, e-trabalho, e-estudo, e-medicina, e-governos, etc.

## Princípios do Direito Digital

### ✓ Princípios Específicos ...

- Princípio do Domínio Público Internacional – entendido como o conjunto dos espaços cujo uso interessa à sociedade internacional como um todo, mesmo que, em certos casos , tais espaços estejam sujeitos à soberania de uma Nação , tal qual são disciplinados pelo Direito Internacional, de entre outros o mar (e suas subdivisões legais), o espaço aéreo, ...
- Princípio da Identidade Reflexa – que prescreve que tudo o que se encontra no ambiente virtual ése destaca que a mensagem passa a ter valor próum “espelho”da existência no mundo real ou físico, com premissa na permissão de regulamentação de identidade no ciberespaço, seja ela de pessoas físicas ou jurídicas, ciber-cidades, e-trabalho, e-estudo, e-medicina, e-governos, etc.

## **Direito. Relacionamento e comunicação**

- O Direito Digital é uma reação jurídica à **virtuaização** das relações humanas
- Antes, numa sociedade pré-industrial, o ser humano se relacionava com 40...50 pessoas...
- Hoje, o ser humano se relaciona com 40...50 pessoas num único e-mail!
- Houve, assim, uma potencialização!
- Tudo começa com a televisão (porém de forma “passiva”)
- Com a Sociedade de Informação , essa lógica muda ...surge interação

**TODOS TEM O DIREITO DE INTERAGIR!**

## Direito, relacionamento e comunicação

- É a virtualização das relações sociais
- Por consequência ... a virtualização das relações jurídicas!
- Daí vem a questão: **quais as regras que devem ser aplicadas a essas novas relações jurídicas?**
- Para isso existem, pelo menos, **quatro correntes doutrinárias...**

## 1ª Corrente ...Liberatória

- Proposta por David Post e David Johnson, com base nas ideias de John Barlow
- Defende uma fronteira entre o direito “real” e o direito “virtual”
- Aqui, todas as regras deverão começar “do zero” e seriam baseadas fundamentalmente no costume.

## 2<sup>a</sup> Corrente ...Da arquitectura da rede

- Proposta por Lawrence Lessig
- O regulamento se basearia no “Código Fonte”
- Assim, as regras seriam definidas por “programadores”, através de linguagens puramente matemáticas, a serem disciplinadas pelo Estado e/ou pelas próprias corporações (nesse caso, há o problema da “manipulação da informação” e, notadamente , do “risco à Liberdade”!)

## 3<sup>a</sup> Corrente ...Do Direito Internacional

- Equiparada o Direito Digital ao Direito Internacional
- Aqui, seriam aceitas as regras já observadas na solução de conflitos transterritoriais
- O grande problema é que o direito Internacional (mesmo possuindo uma grande amplitude) não foi criado para solucionar problemas “virtualizados”

## 4<sup>a</sup> Corrente ...Tradicionalista

- É a corrente mais simplista e dita a aplicação das regras já existentes
  - É relação de consumo? ... aplica-se o CDC
  - É relação civil? ...aplica-se o CC
  - É um conflito penal? ...aplica-se o CP
- Mais uma vez, o problema é a virtualização
- Assim, o que se propõe é a releitura dos princípios e não das regras positivadas

## Relação com outros ramos do Direito

- Direito Constitucional
- Direito Administrativo
- Direito Penal
- Direitos Humanos
- Direito Civil
- Direito Comercial
- Direito Tributário
- Direito de Propriedade Intelectual
- Direito do Trabalho
- Direito do Consumidor
- Direitos Eleitoral
- Direito Processual
- Direito Ambiental

## Novos Institutos Jurídicos

- Documentos electrónicos e Gestão electronica de documentos (GED)
- Segurança da Informação
- Contratos electrónicos
- E-commerce
- Governança Corporativa
- Responsabilidade civil e criminal de empregadores e colaboradores quanto ao uso de ferramentas tecnológicas
- Contratos de uso de licença e registo de Software

## Novos Institutos Jurídicos

- Criminos electrónicos
- Resposta a incidentes
- Fraudes electrónicas
- Concorrência desleal, vazamento de informações, divulgação de segredo e espionage industrial
- Direitos autorais na internet
- Conflitos de marcas versus nomes de domínio
- Cybersquatting e typosquatting



## Nomenclaturas para cibercrimes

- ✓ Crimes virtuais
  - Crimes de internet
- ✓ Crimes Electrónicos (crimes por meios electrónicos)
  - Crimes Digitais
  - Crimes Informáticos (crimes de informática)
    - Crimes de computador (computer crime, criminalidade pelo computador)
- ✓ Crimes Telemáticos

## Classificação dos cibercrimes

- ✓ Quanto à origem
  - Cibercrime interno – quando realizado de dentro do local a ser alvo do crime
  - Cibercrime externo – quando o criminoso pratica um crime sem ter nenhum vínculo com o local a ser alvo do ilícito
- ✓ Quanto à vítima
  - Colectividade (*Adversus omens*)
  - Pessoa determinada (*Adversus in personam*)

## Classificação dos cibercrimes

- ✓ Quanto ao objecto
  - Contra hardware – cibercrime praticado cujo objecto ou resultado do crime é hardware
  - Contra software – cibercrime praticado cujo objecto ou resultado do crime é software
  - Contra informação - cibercrime praticado cujo objecto ou resultado do crime é a informação
  - Diversos – crimes contra bens jurídicos diversos dos sistemas de informação

## Classificação dos cibercrimes

- ✓ Quanto à TIC (Tecnologia da Informação e Comunicação)
  - Cibercrime puro (*crimini versus objectum*) – crime contra o recurso TIC, ou seja , consiste em qualquer conduta ilícita do agente que recai sobre os recursos tecnológicos, informacionais e comunicacionais, seja de forma física ou técnica
  - Cibercrime impuro (*crimini ad objectum*) – crime por intermédio do recurso TIC

## Classificação dos cibercrimes

- ✓ Quanto ao ambiente ou ao meio
  - Cibercrime impróprio ou comum – refere-se ao crime que pode ser cometido tanto no mundo físico ou material como no ciberespaço
  - Cibercrime próprio ou específico – só pode ser cometido no ciberespaço, isto é, deve ser realizado no ambiente virtual, para que a conduta seja concretizada, tendo um tipo penal distinto do tradicional; tanto a acção quanto o resultado da conduta ilícita consumam-se no ciberespaço

## Os “Cibercriminosos”:

- Hacker
- Cracker
- Phreaker
- Insider
- Carder
- Lammer
- Script Kiddies
- Cyberpunks
- Sneakers
- Extortinists
- War drives
- Newbies
- Warezs
- Wannabes
- Ciberterroristas
- Grifers
- Spammers
- Defacer

## Os 10 hackers mais famosos...



- 1º. Kevin Mitnick**. Um dos mais famosos hackers de todos os tempos, Foi o primeiro hacker a entrar para a lista dos 10 criminosos mais procurados pelo FBI.
- 2º. Adrian Lamo**. Na lista de invasões do jovem hacker americano estão os sites da Microsoft, do Yahoo! e do jornal The New York Times.
- 3º. Raphael Gray**. O hacker britânico Raphael Gray, 19 anos, foi condenado por roubar 23 mil números de cartões de crédito, entre eles um de Bill Gates.
- 4º Jonathan James**. Preso aos 16 anos, o hacker invadiu uma das agências Departamento de Defesa americano.
- 5º. Jon Lech Johansen**. Conhecido como DVD Jon, o hacker norueguês ganhou fama após burlar os sistemas de proteção dos DVDs comerciais.
- 6º. Vladimir Levin**. O criminoso russo liderou uma gangue que invadiu computadores do Citibank e desviou US\$ 10 milhões, em 1994.
- 7º. Onel de Guzman**. Com apenas 23 anos, o filipino Onel de Guzman causou um prejuízo de US\$ 10 bilhões com seu vírus "I Love You", que atingiu sistemas de e-mail no mundo todo.
- 8º. Kevin Poulsen**. Ganhou um Porsche num concurso realizado por uma rádio americana. O 102º ouvinte que telefonasse para a emissora, levava o carro. Poulsen invadiu a central.
- 9º. Robert Morris**. O americano, filho do cientista chefe do Centro Nacional de Segurança Computacional dos EUA, espalhou o primeiro worm que infectou milhões de computadores e fez grande parte da Internet entrar em colapso, em 1988.
- 10º. David L. Smith**. Com o vírus Melissa, o programador conseguiu derrubar servidores de grandes empresas, como Intel e Microsoft.

# Actividade



# Actividade 3 – TG1

## **TRABALHO EM GRUPO 1:**

1. Das quatro correntes doutrinárias relacionadas com o Direito Digital, diga com qual delas se identifica e porquê?
2. Indique em que redes sociais cada membro do grupo participa e identifique a(s) rede(s) social(ais) que mais participam e justifique a adesão.
3. Efectuem o levantamento da legislação moçambicana, relacionada ao Direito Digital

Nota: Recomenda-se a consulta dos sites das seguintes entidades: Ministério de Ciência e Tecnologia Ensino Superior (MCTES); Instituto Nacional de Tecnologias de Informação e Comunicação (INTIC); Instituto Nacional de Comunicações de Moçambique (INCM); Instituto Nacional do Governo Electrónico (INAGE)

4. Dissertem sobre o conceitos: *Cybersquatting* e *Typosquatting* (sugere-se se sejam localizadas e na internet algumas situações que ilustram eventuais situações de *Cybersquatting* e *Typosquatting*)
5. Elaborem uma apresentação em power point (para cerca de 15mim), abordando os aspectos discutidos neste trabalho (perguntas 1 a 5)

**Data de Entrega: 20/03/2023**

# Fundamentos de Segurança Redes



- ✓ O que é segurança de rede?
- ✓ Por que a segurança de rede é importante?
- ✓ Confidencialidade, integridade e disponibilidade (CIA)
- ✓ Domínios da Infraestrutura Típica de TI
- ✓ Quais são os tipos de segurança de rede?
- ✓ Principais ameaças à segurança de rede nos últimos anos

## O que é Segurança de Rede:

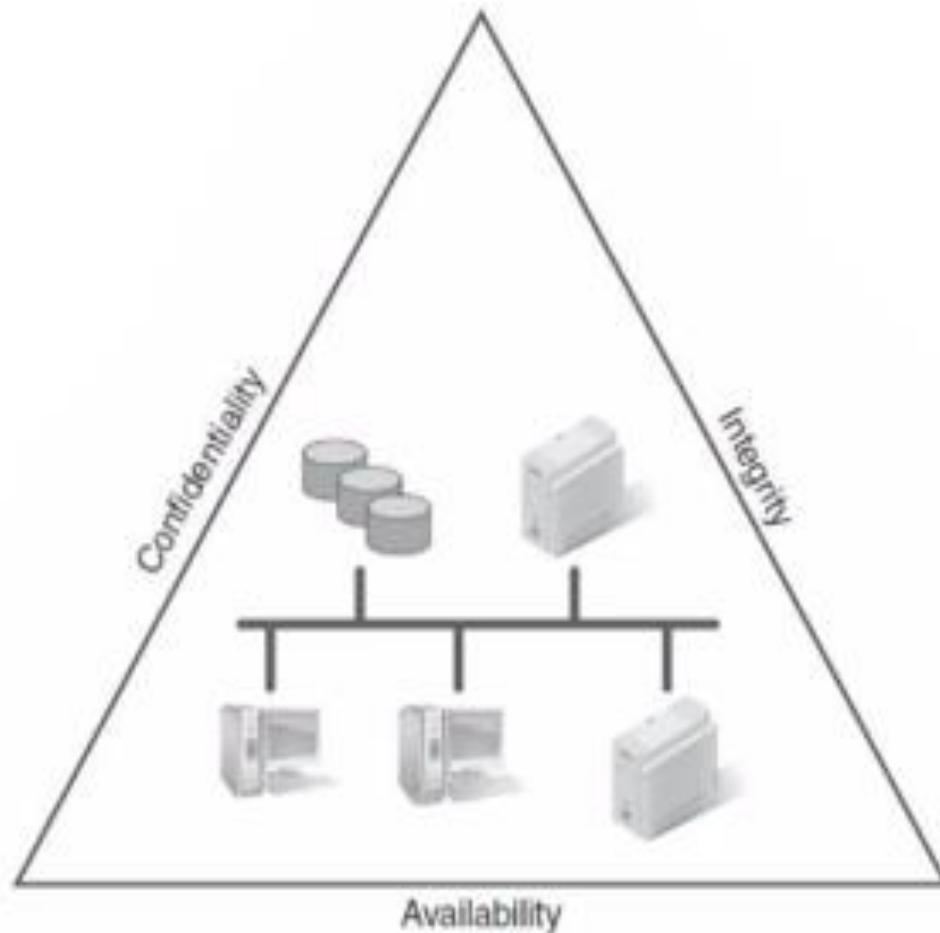
- ✓ A segurança de rede é uma combinação de tecnologias, dispositivos e processos projetados para proteger a infraestrutura de rede de uma organização contra acesso não autorizado, exploração de seus recursos corporativos, divulgação imprópria e negação de serviços.
- ✓ A segurança de rede é um componente crítico que uma organização deve implementar para proteger seus interesses e operar com eficiência.
- ✓ Os métodos que uma empresa implementa para proteger sua rede podem variar de uma organização para outra.



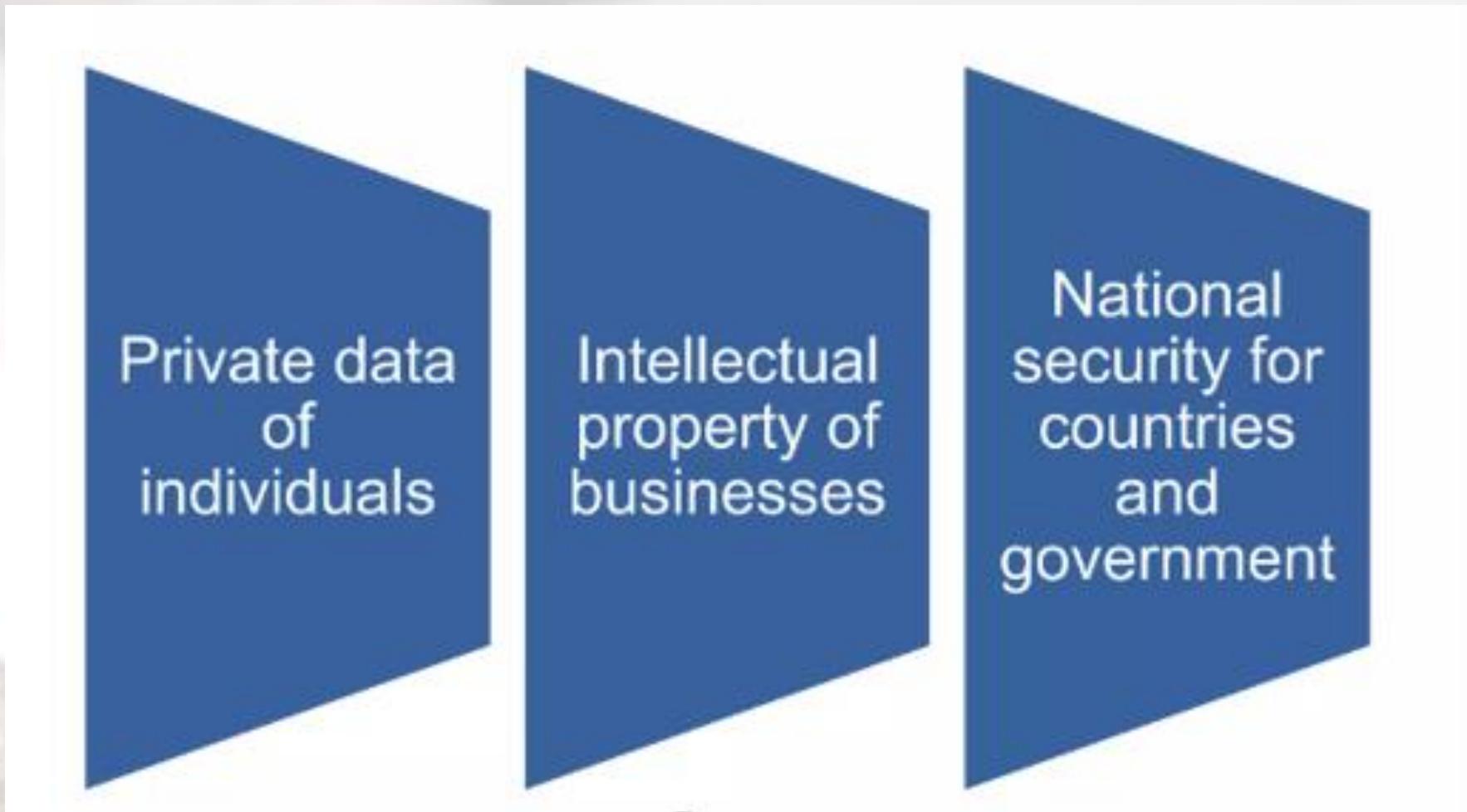
## Porque a Segurança de Rede é Importante?

- ✓ A segurança da rede é importante porque mantém os dados confidenciais protegidos contra ataques cibernéticos e garante que a rede seja utilizável e confiável.
- ✓ Oferecer um sistema de segurança de rede pode trazer a seus clientes a confiança de saber que seus activos mais valiosos - seus sistemas de computador, redes e dados - estão seguros, protegidos e protegidos contra ataques e utilizadores não autorizados de dentro ou fora de sua empresa.

## Confidencialidade, Integridade e Disponibilidade (CIA)



## Confidencialidade:



## Medições de tempo de Disponibilidade

■ Uptime

Downtime

Availability [ $A = (\text{Total Uptime}) / (\text{Total Uptime} + \text{Total Downtime})$ ]

Mean time to failure (MTTF)

Mean time to repair (MTTR)

Mean time between failures (MTBF)

Recovery time objective (RTO)

## Riscos, Ameaças, Vulnerabilidades

Eavesdropping

Call control

Impersonation

Toll fraud

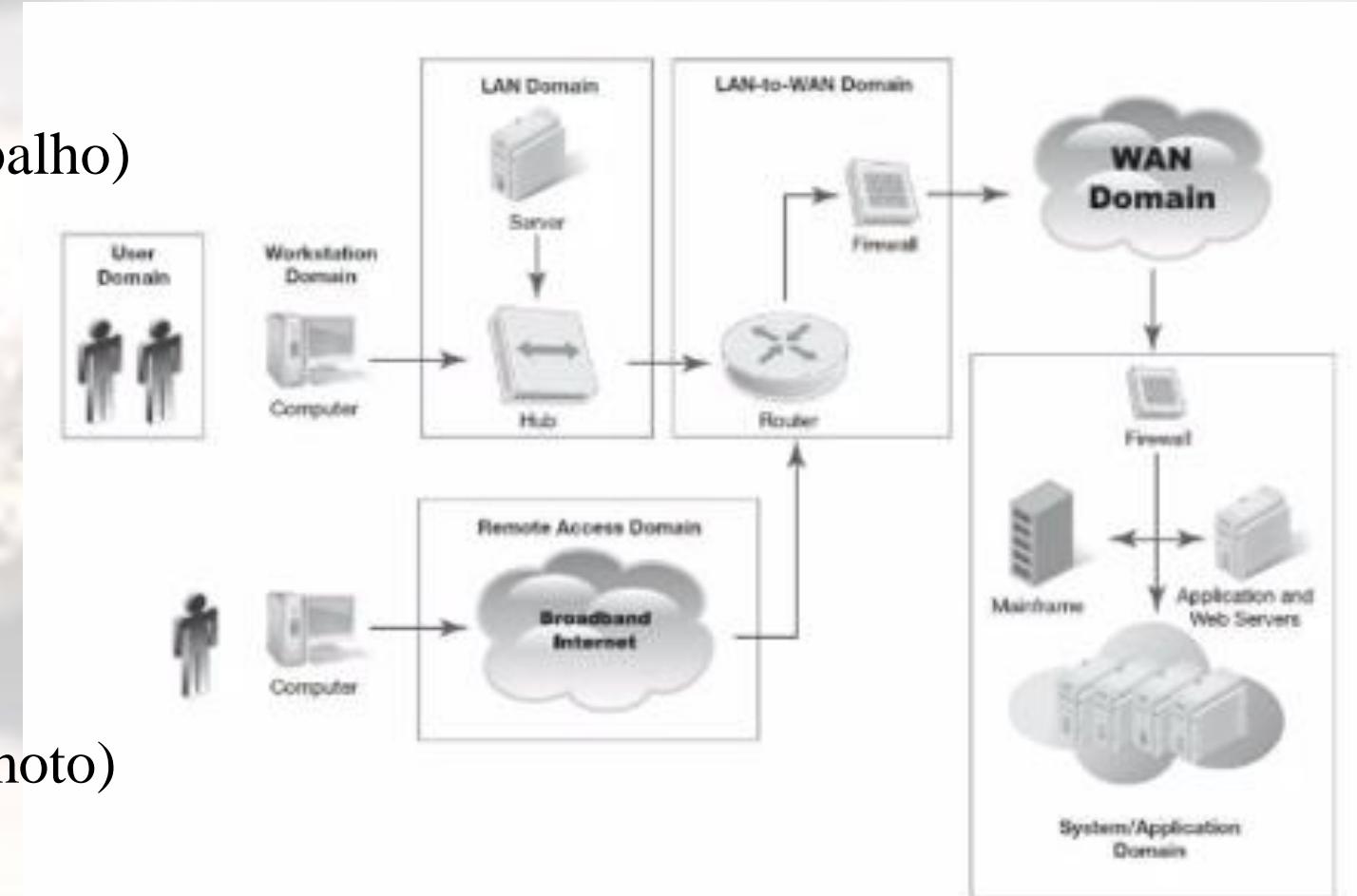
Brute-force password attacks

Denial of Service (DoS) attacks



## Domínios da Infraestrutura Típica de TI

- ✓ User Domain (utilizadores)
- ✓ Workstation Domain (Estação de trabalho)
- ✓ LAN Domain
- ✓ LAN-to-WAN Domain
- ✓ WAN Domain
- ✓ Remote Access Domain (Acesso Remoto)
- ✓ System/Application Domain



## User Domain

### Funções e Tarefas

- ✓ Os usuários podem acessar sistemas, aplicativos e dados dependendo de seus direitos definidos User Domain (utilizadores)

### Responsabilidades

- ✓ Os funcionários são responsáveis pelo uso dos ativos de TI

### Accountability

- ✓ O departamento de RH é responsável por implantar verificações adequadas de antecedentes dos funcionários

## Ameaças comuns no *User Domain*

- ✓ Falta de conscientização do utilizador
- ✓ Apatia do utilizador em relação às políticas
- ✓ Política de segurança violada pelo utilizador
- ✓ Utilizador inserindo CD/USB com arquivos pessoais
- ✓ Utilizador baixando fotos, músicas ou vídeos
- ✓ Utilizador destruindo sistemas, aplicativos e dados
- ✓ Funcionário descontente atacando a organização ou cometendo sabotagem
- ✓ Chantagem ou extorsão de funcionários

## LAN Domain

### Funções e Tarefas

- ✓ Inclui componentes de rede física e configuração lógica de serviços para utilizadores

### Responsabilidades

- ✓ O grupo de suporte LAN é responsável pelos componentes físicos e elementos lógicos

### Accountability

- ✓ O dever do Administrador da LAN é maximizar o uso e a integridade dos dados dentro do Domínio da LAN

## Ameaças comuns no *LAN Domain*

- ✓ Acesso físico não autorizado à LAN
- ✓ Acesso não autorizado aos sistemas, aplicativos e dados
- ✓ Vulnerabilidades de software de aplicativo LAN Server
- ✓ Vulnerabilidades de software de aplicativo de servidor LAN e atualizações de patch de software
- ✓ Utilizadores desonestos em WLANs
- ✓ Confidencialidade de dados em WLANs
- ✓ Diretrizes e padrões de configuração do LAN Server

## LAN-to-WAN Domain

### Funções e Tarefas

- ✓ Inclui as peças físicas e o design lógico dos dispositivos de segurança. As partes físicas precisam ser gerenciadas para facilitar o acesso ao serviço

### Responsabilidades

- ✓ Componentes físicos, elementos lógicos e aplicação dos controlos de segurança definidos

### Accountability

- ✓ Certifique-se de que as políticas, padrões, procedimentos e diretrizes de segurança de domínio LAN-to-WAN sejam usados

## Ameaças comuns no *LAN-to-WAN Domain*

- ✓ Sondagem não autorizada e verificação de portas
- ✓ Acesso não autorizado
- ✓ Vulnerabilidade do roteador IP, firewall e sistema operacional do dispositivo de rede
- ✓ Download de anexos de tipo de arquivo desconhecido de fontes desconhecidas
- ✓ Anexos de e-mail desconhecidos e links de URL incorporados recebidos por usuários locais

## WAN Domain

### Funções e Tarefas

- ✓ Permite aos utilizadores o máximo de acesso possível, certificando-se de que tudo o que entra e sai é seguro

### Responsabilidades

- ✓ Componentes físicos e elementos lógicos

### Accountability

- ✓ Manter atualizado, fornecer suporte técnico e garantir que a empresa atenda às políticas, padrões, procedimentos e diretrizes de segurança

## Ameaças comuns no *WAN Domain* (Internet)

- ✓ Dados abertos, públicos e acessíveis
- ✓ A maior parte do tráfego sendo enviado como texto não criptografado
- ✓ Vulnerável a espionagem
- ✓ Vulnerável a ataques maliciosos
- ✓ Vulnerável a ataques de negação de serviço (DoS) e negação de serviço distribuído (DDoS)
- ✓ Vulnerável à corrupção de informações/dados
- ✓ Aplicativos TCP/IP inseguros

## Ameaças comuns no *WAN Domain* (Conectividade)

- ✓ Combinação de tráfego Wan IP no mesmo roteador e infraestrutura do provedor de serviços
- ✓ Manter alta disponibilidade de serviço WAN
- ✓ Usando aplicativos e protocolos de gerenciamento de rede SNMP de forma maliciosa (ICMP, Telnet, SNMP, DNS, etc.)
- ✓ Alarmes SNMP e monitoramento de segurança 24 x 7 x 365

## Remote Access Domain

### Funções e Tarefas

- ✓ Conecte utilizadores móveis a seus sistemas de TI por meio da Internet pública

### Responsabilidades

- ✓ Manter, atualizar e solucionar problemas de hardware e conexão lógica de acesso remoto

### Accountability

- ✓ Certifique-se de que os planos, padrões, métodos e diretrizes de segurança do domínio de acesso remoto sejam usados

## Ameaças comuns no *Remote Access Domain*

- ✓ Ataques de força bruta a ID e senhas de utilizadores
- ✓ Ataques de controlo de acesso a várias tentativas de logon
- ✓ Acesso remoto não autorizado a sistemas, aplicativos e dados de TI
- ✓ Dados confidenciais comprometidos remotamente
- ✓ Vazamento de dados em violação dos padrões de classificação de dados

## Elo mais fraco na segurança de uma infraestrutura de TI

O utilizador é o elo mais fraco em segurança

Estratégias para reduzir o risco

- ✓ Verifique cuidadosamente o histórico dos candidatos a emprego
- ✓ Avalie a equipe regularmente
- ✓ Rotacione o acesso a sistemas, aplicativos e dados confidenciais entre os cargos da equipe
- ✓ Teste o aplicativo e o software e analise a qualidade
- ✓ Revise regularmente os planos de segurança
- ✓ Realizar auditorias anuais de controle de segurança

# Actividade



## **TRABALHO EM GRUPO 2:**

1. Selecione uma das ferramentas de análise de segurança de websites abaixo indicadas (ou uma outra da sua preferência) e prepare uma demonstração das suas funcionalidades

- Sucuri Site Check
- Mozilla Observatory
- SSLtrust
- WPScan
- Quttra
- Site Guarding
- CWatch
- Scanurl
- HackerCombar

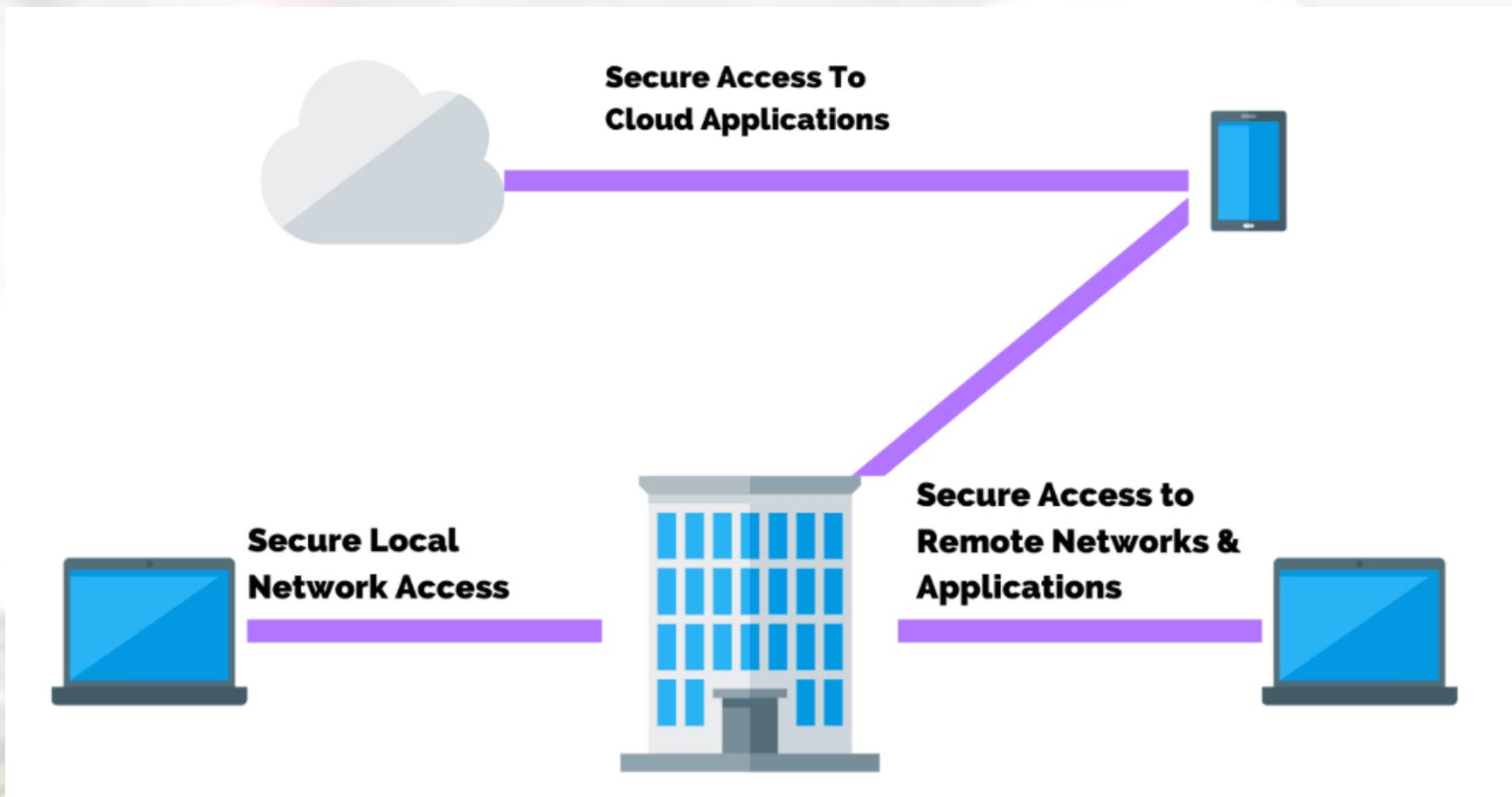
**Data de Entrega: 27/03/2023**



## **Tipos de Segurança de Redes:**

- ✓ Controlo de Acesso à Rede
- ✓ Políticas de segurança de rede
- ✓ Segurança do Aplicativo
- ✓ Gestão de patches de vulnerabilidade
- ✓ Teste de penetração de rede
- ✓ Prevenção de perda de dados
- ✓ Software antivírus
- ✓ Detecção e Resposta de Endpoint (EDR)
- ✓ Segurança de e-mail
- ✓ Segurança em redes sem fio
- ✓ IDS/IPS
- ✓ Segmentação de rede
- ✓ SIEM
- ✓ Segurança da Web
- ✓ Autenticação Multifator (MFA)
- ✓ Rede Privada Virtual (VPN)

## Controlo de Acesso à Rede (*Network Access Control*):



## **Controlo de Acesso à Rede (*Network Access Control*):**

- ✓ Com as organizações adoptando as políticas BYOD (*Bring Your Own Device*), é essencial ter uma solução que forneça os recursos de visibilidade, controlo de acesso e conformidade necessários para fortalecer sua infraestrutura de segurança de rede.
- ✓ O Network Access Control ou NAC é uma solução de rede que permite que apenas dispositivos de endpoint compatíveis, autenticados e confiáveis acedam recursos e infraestrutura de rede.
- ✓ Um sistema NAC utiliza o controlo de endereço MAC e o protocolo SNMP (*Simple Network Management Protocol*) para negar acesso à rede a dispositivos não compatíveis, colocá-los em uma área de quarentena ou dar-lhes apenas acesso restrito a recursos de computação, evitando que nós inseguros infectem a rede.
- ✓ Uma solução NAC também pode isolar convidados de sua rede interna, identificando todos os dispositivos inseridos nas portas do switch de rede e pode desabilitar remotamente um dispositivo invasor da porta do switch sem envolver o suporte técnico.

# Fundamentos de SR

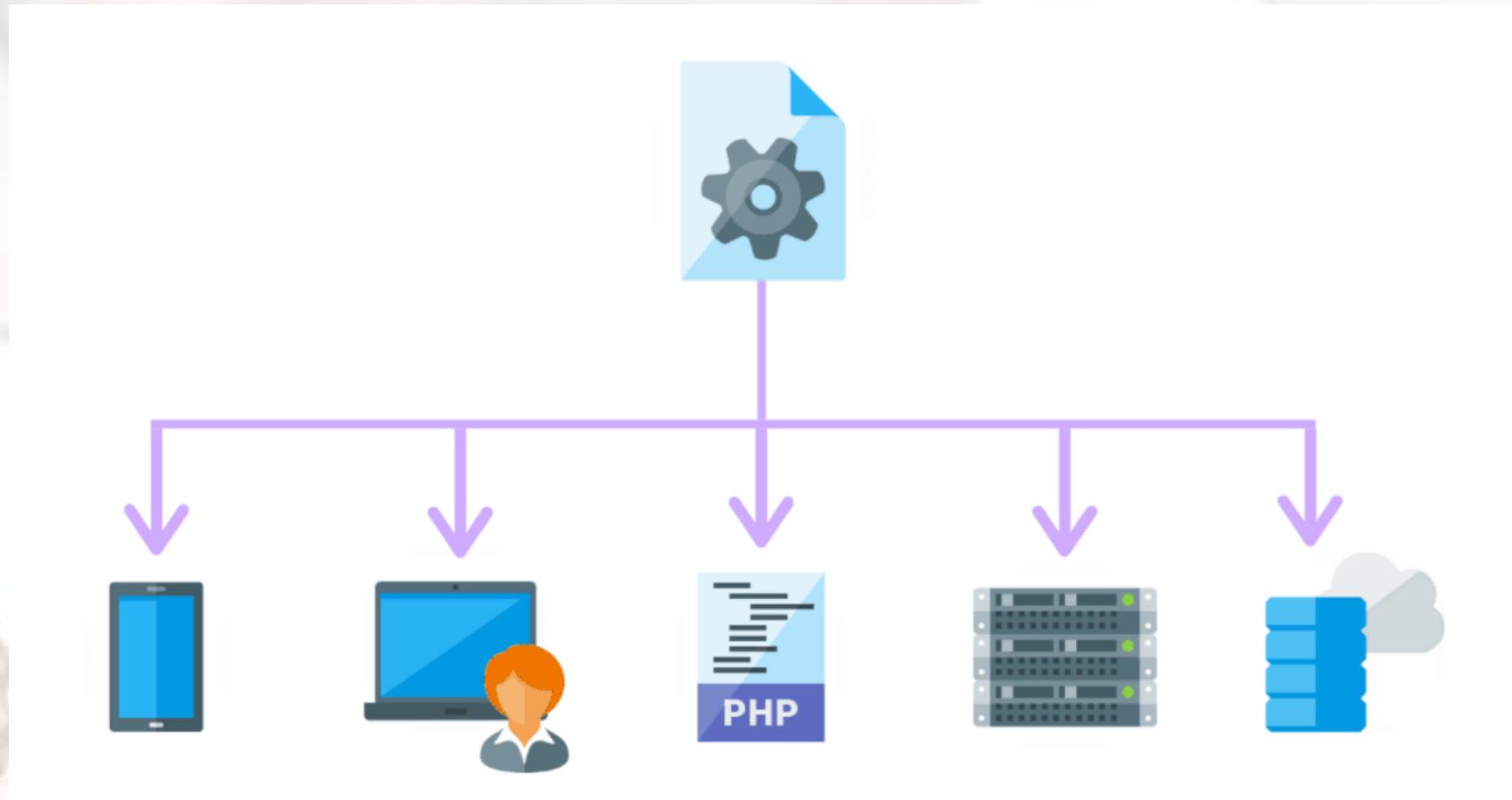
## Controlo de Acesso à Rede (*Network Access Control*):

PARAMETER	NOC	SOC
Full Form	Network Operations Center	Security Operations Center
Terminology	Used to handle challenges related to managing, monitoring, and controlling the networks in customer IT ecosystem	Tracks threats to infrastructure making attempts to use vulnerability and get inside of a network.
Key Role	To meet service level agreements and manage incidents to achieve maximum uptime.	To protect intellectual property and secure sensitive customer information
Objectives	To monitor performance	To monitor quality
Technology	Real-time data access	Real-time and historical data access
Tools	Fault, trouble and performance monitoring software.	Service quality, customer experience and marketing software.
Skills	<ul style="list-style-type: none"><li>• Network infrastructure</li><li>• Data analytics,</li><li>• troubleshooting and</li><li>• technology know-how.</li></ul>	<ul style="list-style-type: none"><li>• Security infrastructure</li><li>• Service modelling</li><li>• data interpretation</li><li>• communication.</li></ul>
Metrics	Reactive approach	Proactive approach
Business impact	Operational	Strategic
Size	80-500+ engineers	10-100 engineers

## Controlo de Acesso à Rede (*Network Access Control*):

- ✓ O foco principal de um SOC (*Security Operations Center*) é a segurança da informação e dos dados. Ele deve identificar as ameaças de segurança do ambiente de TI da sua organização. O trabalho do SOC é monitorar e analisar a infraestrutura de TI e, quando uma anormalidade for detectada, o SOC deve se mover rapidamente para escalar, determinar a natureza da ameaça e, em seguida, resolvê-la.
- ✓ O NOC (*Network Operations Center*), por sua vez, foca no monitoramento da rede da sua empresa. A equipe garante que o ambiente de rede esteja atendendo aos requisitos de desempenho e disponibilidade. Se a rede está funcionando de forma ineficiente, o trabalho do NOC é determinar o motivo.
- ✓ Na prática, a função do NOC é considerada operacional, enquanto o SOC possui um impacto estratégico nos negócios. Desta forma, a operação e o gestão de ambos os grupos são diferentes.

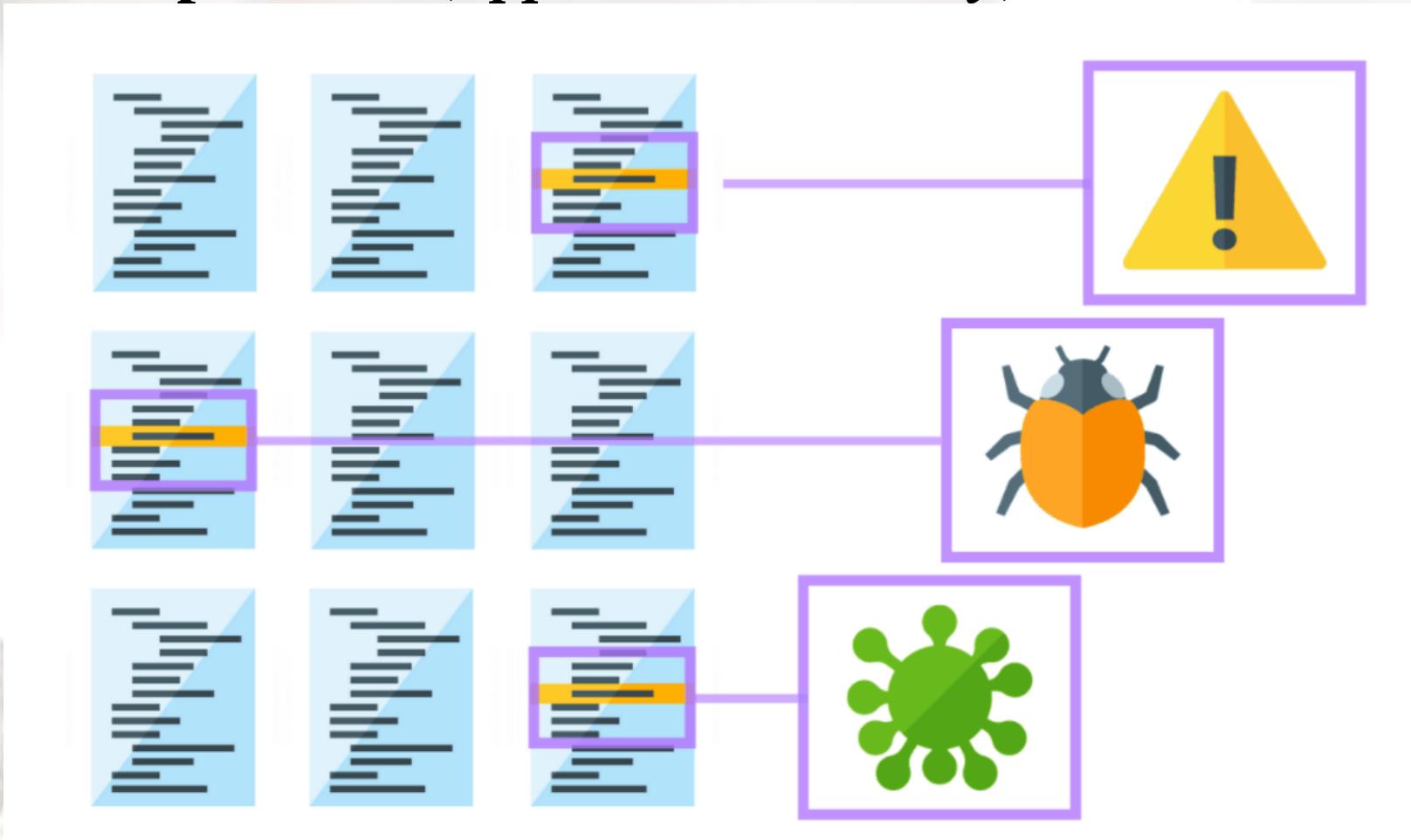
**Políticas de segurança de rede (*Network Security Policies*):**



## **Políticas de segurança de rede (*Network Security Policies*):**

- ✓ Uma política de segurança de rede é um conjunto de práticas e procedimentos padronizados que descreve as regras de acesso à rede, a arquitectura da rede e determina como as políticas são aplicadas.
- ✓ Ter uma política de segurança de rede é importante porque informa aos funcionários de uma organização os requisitos para proteger os activos dentro da infraestrutura. Esses activos assumem várias formas, como senhas, documentos ou até mesmo servidores.
- ✓ Políticas também estabelecem directrizes para adquirir, configurar e auditar sistemas e redes de computadores.
- ✓ Uma política de segurança de rede que seja facilmente interpretada e aplicada pode proteger a rede contra perda accidental ou intencional de dados, diminuir o risco de ataques cibernéticos e preservar a integridade dos dados corporativos.

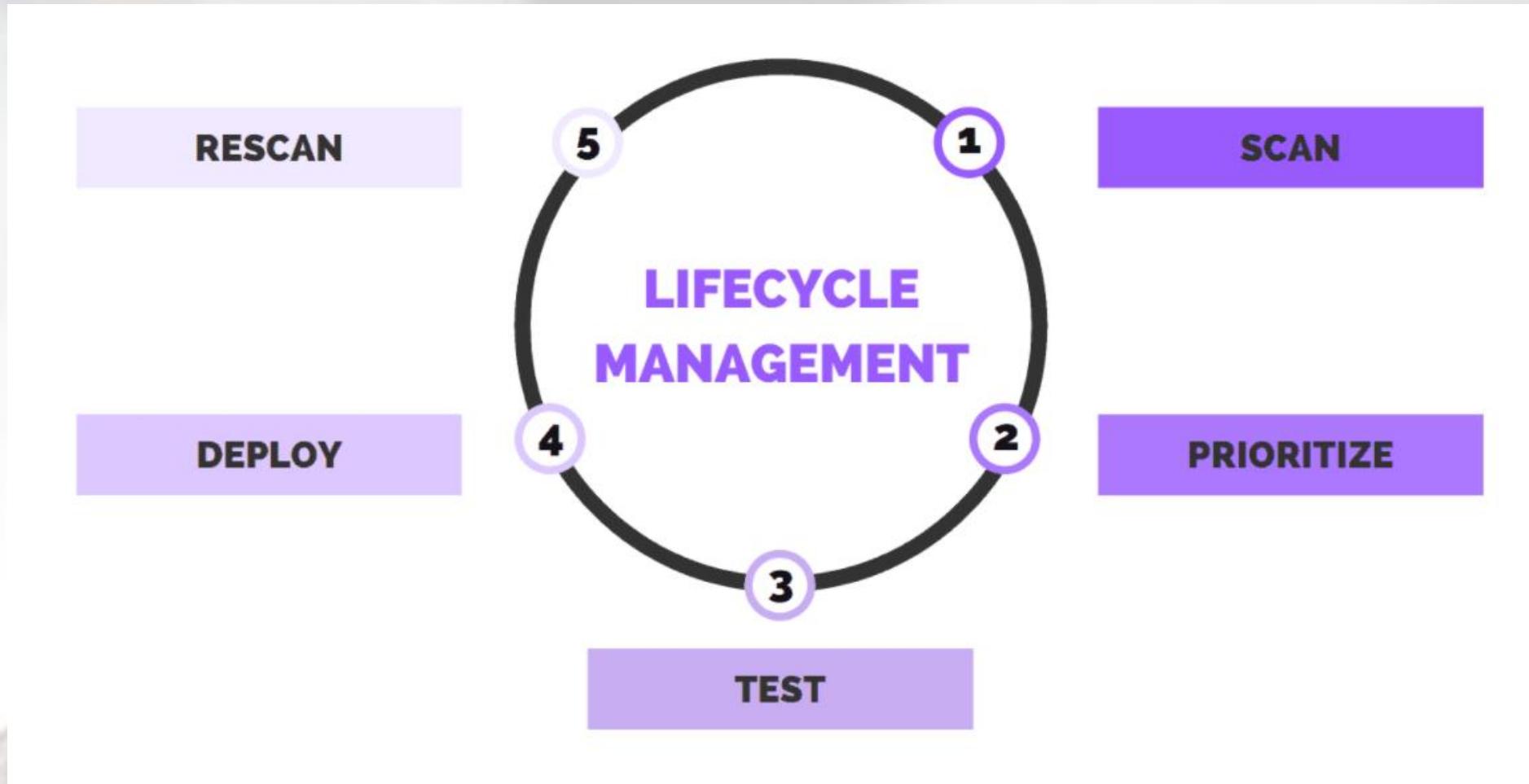
## Segurança do Aplicativo (*Application Security*):



## **Segurança do Aplicativo (*Application Security*):**

- ✓ A segurança de aplicativos é o processo de desenvolver, adicionar e testar recursos de segurança em aplicativos para evitar vulnerabilidades de segurança contra ameaças como acesso e modificação não autorizados.
- ✓ De acordo com o relatório State of Software Security da Veracode, 83% dos 85.000 aplicativos testados tinham pelo menos uma falha de segurança.
- ✓ Muitos tinham muito mais, pois sua pesquisa encontrou um total de 10 milhões de falhas e 20% de todos os aplicativos tinham pelo menos uma falha de alta gravidade.
- ✓ É importante que as organizações realizem testes de segurança de aplicativos de rotina para identificar e mitigar falhas no código.
- ✓ Isso impedirá que invasores cibernéticos comprometam ou explorem aplicativos da Web críticos

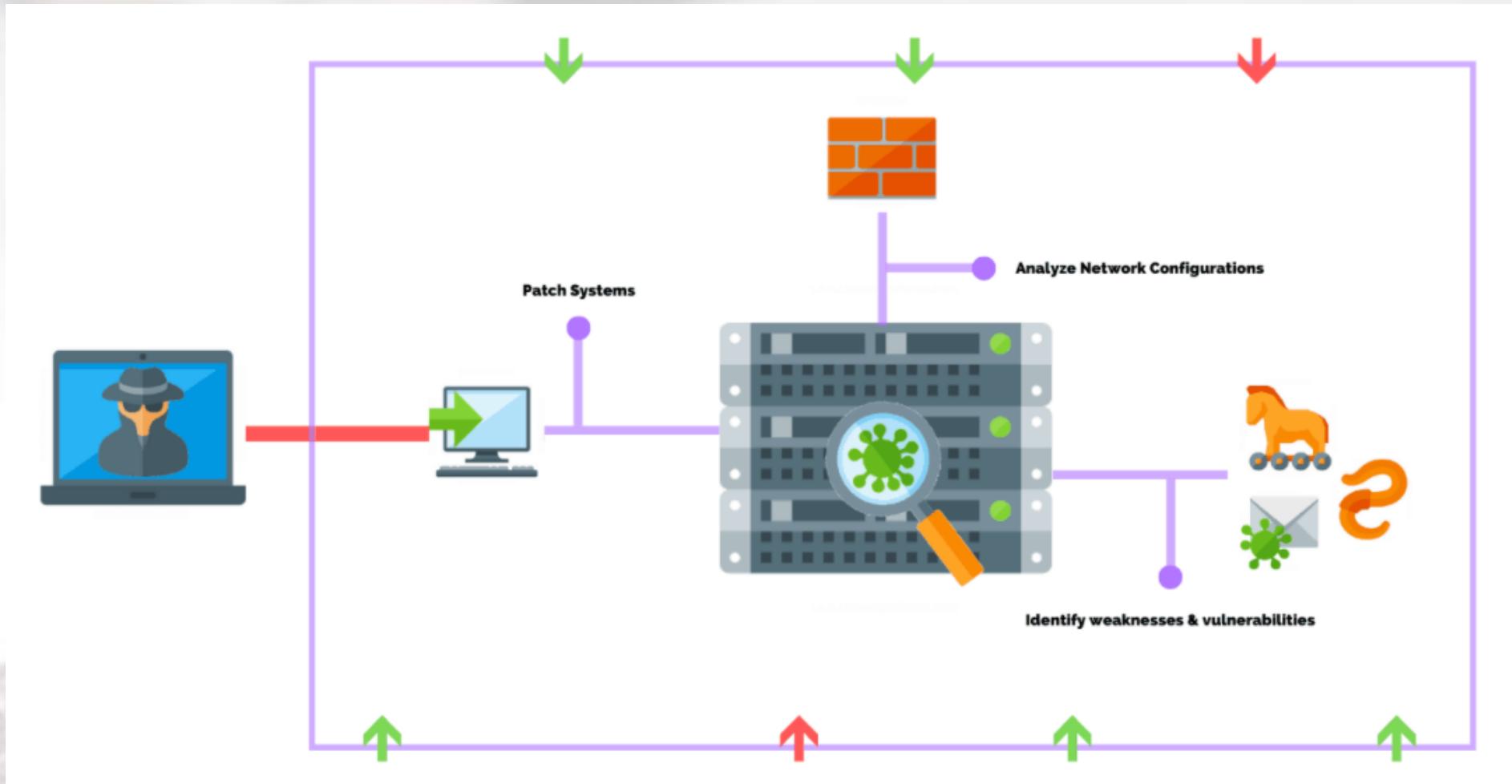
## Gestão de patches de vulnerabilidade (*Vulnerability Patch Management*):



## **Gestão de patches de vulnerabilidade (*Vulnerability Patch Management*):**

- ✓ A gestão de patches de vulnerabilidade é um processo contínuo de identificação, priorização, correção e relatórios sobre vulnerabilidades de segurança em sistemas.
- ✓ Os activos na rede são descobertos, categorizados e relatados para corrigir vulnerabilidades de segurança nos sistemas de destino.
- ✓ A gestão de patches de vulnerabilidade é fundamental hoje porque os invasores estão constantemente rastreando a Internet em busca de vulnerabilidades a serem exploradas – e aproveitando vulnerabilidades antigas que não foram corrigidas em sistemas corporativos.

## Teste de penetração de rede (*Network Penetration Testing*):



## **Teste de penetração de rede (*Network Penetration Testing*):**

- ✓ O teste de penetração de rede é uma tentativa de medir e avaliar a segurança de uma infraestrutura de TI tentando explorar vulnerabilidades com segurança.
- ✓ Essas vulnerabilidades podem existir em sistemas operacionais, falhas de serviços e aplicativos, configurações de firewall impróprias ou comportamento arriscado do utilizadores final.
- ✓ A principal razão pela qual o teste de penetração é importante para o programa de segurança de rede de uma organização é que ele ajuda o pessoal a aprender como lidar com ataques cibernéticos de uma entidade maliciosa.
- ✓ O teste de penetração também serve para examinar se as políticas de segurança de uma organização são funcionais e eficazes na dissuasão de ataques.

## **Teste de penetração de rede (*Network Penetration Testing*):**

- ✓ O teste de penetração de rede é uma tentativa de medir e avaliar a segurança de uma infraestrutura de TI tentando explorar vulnerabilidades com segurança.
- ✓ Os testes de penetração se enquadram em **duas grandes categorias:**
  - Teste de penetração de endpoint
  - Teste de penetração de rede
- ✓ Enquanto o teste de penetração de endpoint analisa os pontos fracos em sistemas operacionais e software, o teste de penetração de rede visa pontos fracos de comunicação, como portas abertas. Embora o objectivo final seja chegar a um endpoint, todo tipo de ataque de hacker precisa passar por uma rede para atingir um alvo.
- ✓ Mesmo após a violação de um endpoint, os ataques à rede não param. Muitos ataques de rede comuns só podem ser executados dentro da rede. Esses ataques de rede secundários visam mover-se por uma rede para pesquisar ou infectar outros endpoints.
- ✓ Portanto, a categoria de ferramentas de teste de penetração de rede inclui sistemas para colocar o invasor em uma rede e sistemas para documentar a rede e investigar maneiras de chegar aos terminais.

## Portas mais comuns

Os números de porta são divididos em três faixas: As portas bem conhecidas, os pontos registrados, e as portas dinâmicas ou privadas. As portas bem conhecidas são as de 0 a 1023. Os exemplos incluem:

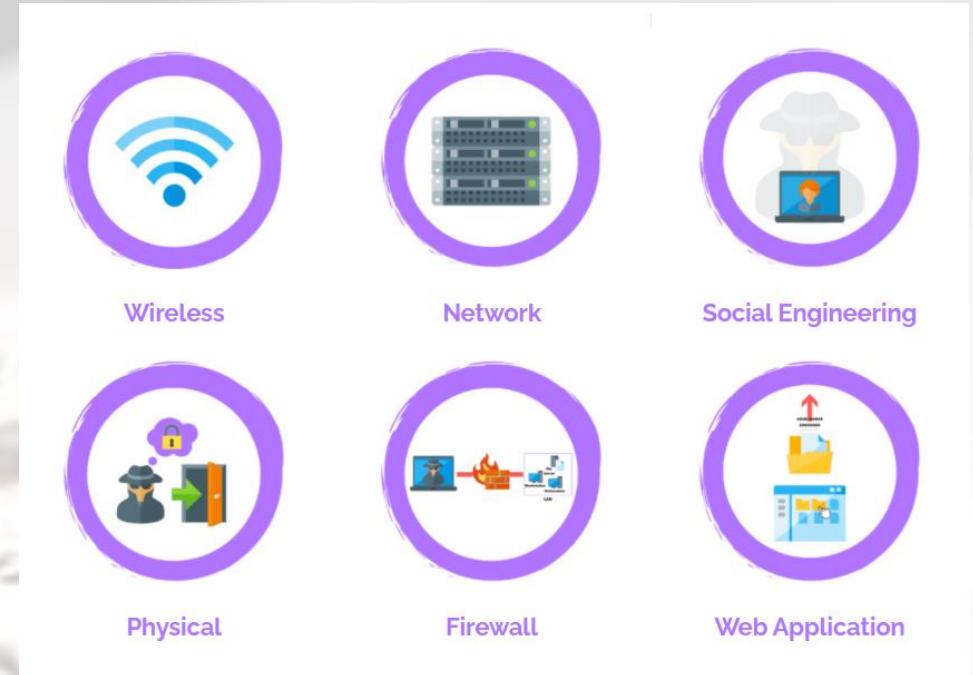
- 20 & 21: File Transfer Protocol (FTP)
- 22: Secure Shell (SSH)
- 23: Telnet remote login service
- 25: Simple Mail Transfer Protocol (SMTP)
- 53: Domain Name System (DNS) service
- 80: Hypertext Transfer Protocol (HTTP) used in the World Wide Web
- 110: Post Office Protocol (POP3)
- 119: Network News Transfer Protocol (NNTP)
- 143: Internet Message Access Protocol (IMAP)
- 161: Simple Network Management Protocol (SNMP)
- 443: HTTP Secure (HTTPS)

# Fundamentos de SR

## Teste de penetração de rede (*Network Penetration Testing*):

✓ Os diferentes **tipos de testes de penetração** incluem:

- Sserviços de rede (network services),
- Aplicativos, (applications),
- lado do cliente (client side),
- Sem fio (wireless),
- Engenharia social (social engineering)
- Física ( physical)



✓ Um teste de penetração pode ser realizado externamente ou internamente para simular diferentes vetores de ataque.

✓ As diferentes **abordagens para testes de penetração** incluem:

- Caixa preta (Black box)
- Caixa branca (White box), also called clear box testing, glass box testing, or internal penetration testing
- Caixa Cinza (Gray box)

## Teste de penetração de rede (*Network Penetration Testing*):

✓ Algumas ferramentas mais populares :

- **1. Netsparker** - O Netsparker Security Scanner é um aplicativo da Web e pode identificar tudo, desde scripts entre sites até injeção de SQL. Os desenvolvedores podem usar essa ferramenta em sites, serviços da web e aplicativos da web
- **2. Wireshark** - Conhecido como Ethereal 0.2.0, o Wireshark é um analisador de rede premiado com 600 autores. Com este software, você pode capturar e interpretar rapidamente os pacotes de rede. A ferramenta é de código aberto e está disponível para vários sistemas, incluindo Windows, Solaris, FreeBSD e Linux.
- **3. Metasploit** – Considerada a estrutura de automação de testes de penetração mais usada no mundo. O Metasploit ajuda equipes profissionais a verificar e gerir avaliações de segurança, melhorar a conscientização e armar e capacitar os defensores. É útil para verificar a segurança e identificar falhas, configurando uma defesa. Um software de código aberto, esta ferramenta permitirá que um administrador de rede invada e identifique pontos fracos fatais. Os hackers iniciantes usam essa ferramenta para desenvolver suas habilidades. A ferramenta fornece uma maneira de replicar sites para engenheiros sociais.

## Teste de penetração de rede (*Network Penetration Testing*):

✓ Algumas ferramentas mais populares :

- **4. BeEF** - É mais adequada para verificar um navegador da web. Adaptado para combater ataques na web e pode beneficiar clientes móveis. BeEF significa Browser Exploitation Framework e usa o GitHub para localizar problemas. O BeEF foi projectado para explorar os pontos fracos além do sistema do cliente e do perímetro da rede..
- **5. John The Ripper Password Cracker ( Decifrador de senhas)** - As senhas são uma das vulnerabilidades mais proeminentes. Os invasores podem usar senhas para roubar credenciais e entrar em sistemas confidenciais. John the Ripper é a ferramenta essencial para quebra de senhas e fornece uma variedade de sistemas para esse fim. É um software de código aberto gratuito.
- **6. Aircrack NG** é projetado para quebrar falhas em conexões sem fio, capturando pacotes de dados para um protocolo eficaz na exportação através de arquivos de texto para análise. Enquanto o software parecia abandonado em 2010, o Aircrack foi actualizado novamente em 2019.

## **Teste de penetração de rede (*Network Penetration Testing*):**

✓ Algumas ferramentas mais populares :

- **7. Kali Linux** - O software de teste de penetração avançado Kali Linux é uma distribuição Linux usada para testes de penetração. Muitos especialistas acreditam que esta é a melhor ferramenta para este tipo de testes. No entanto, é preciso ter habilidades no protocolo TCP/IP para obter o maior benefício.
- **Outras Ferramentas:** Burp Suite Pen Tester; Acunetix Scanner; Ettercap; W3af; Nessus; (SET) Social Engineer Toolkit; Zed Attack Proxy; Wapiti

**Lembre-se de que uma das melhores técnicas para defender sua estrutura de TI é usar o teste de penetração de forma proactiva. Avalie sua segurança de TI procurando e descobrindo problemas antes que invasores em potencial o façam!**

# Actividade



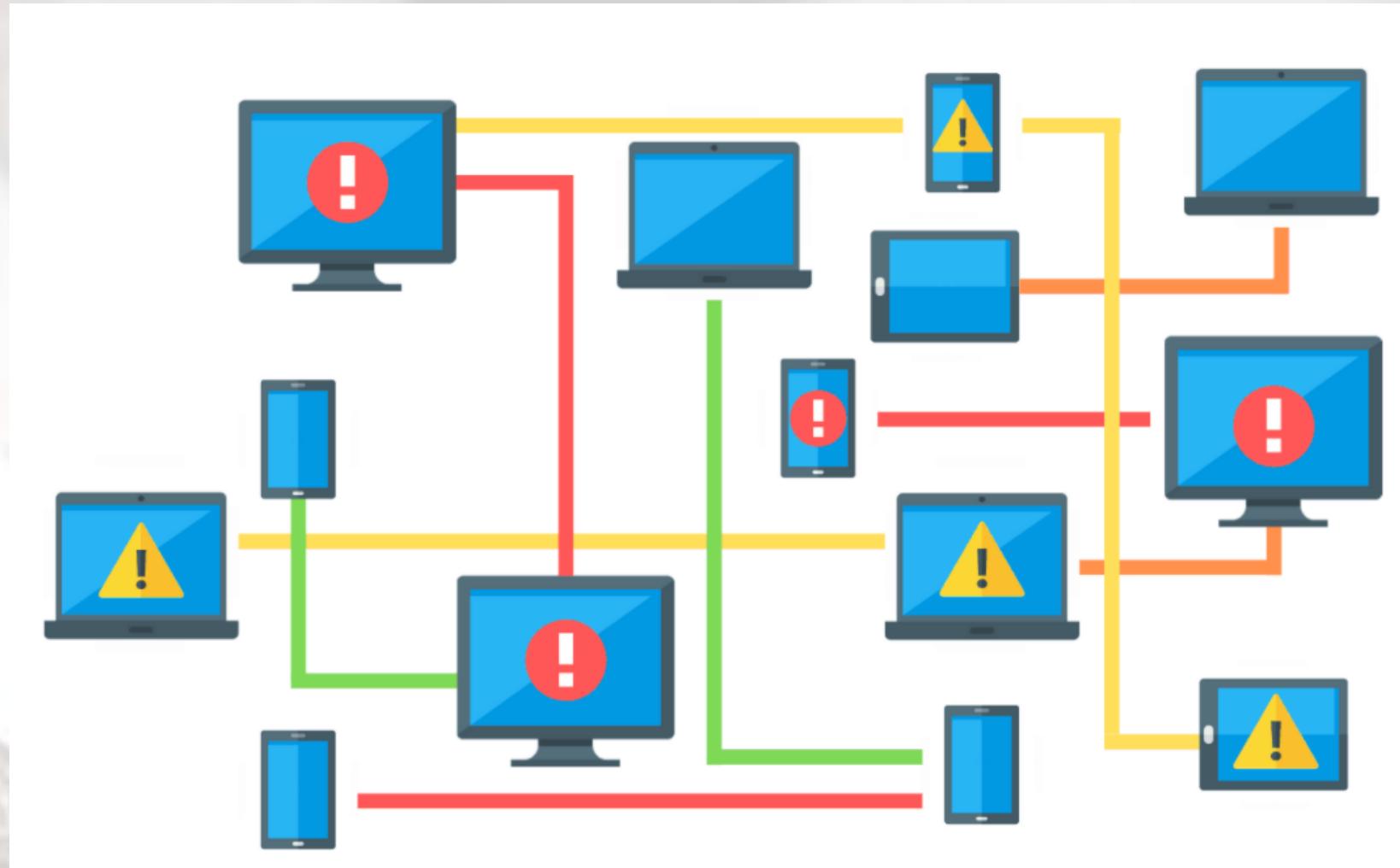
## **TRABALHO EM GRUPO 3:**

1. Descreva cada um dos conceitos indicados nos seguintes slides:
  - Slide 106, com o título: os “Cibercriminosos”
  - Slide 116, referentes à Medição de Tempo de Disponibilidade.
2. Prepare uma apresentação demonstrando o funcionamento de uma das ferramentas referenciadas nos slides 150, 151 e 152 (ou uma outra a sua escolha) – máximo 30 minutos.

**Data de Entrega: 17/04/2023**



## Prevenção de perda de dados (*Data Loss Prevention*):



## **Prevenção de perda de dados (*Data Loss Prevention*):**

- ✓ A prevenção de perda de dados é definida como uma estratégia que detecta possíveis violações de dados ou transmissões de ex-filtragem de dados e as previne monitorando, detectando e bloqueando dados confidenciais durante o uso (acções de endpoint), em movimento (tráfego de rede) e em repouso (armazenamento de dados).
- ✓ A principal razão pela qual o DLP é importante porque ajuda a detectar ou evitar a exposição não intencionais de dados sensíveis.
- ✓ Dependendo do software DLP e da configuração da política, o DLP pode alertar o utilizador final por meio de pop-up ou mensagem de e-mail.
- ✓ Essa personalização impede o vazamento de dados, seja a actividade accidental ou maliciosa.

## **Prevenção de perda de dados (*Data Loss Prevention*):**

- ✓ O sucesso de um programa DLP depende de uma estratégia e implantação de DLP bem planeadas. A liderança executiva deve fornecer orientação e definir as expectativas para o programa geral de DLP.
- ✓ Também é importante conhecer e entender o modelo de negócios da organização. O conhecimento de onde os dados mais críticos são armazenados e como são acedidos é fundamental para o sucesso da estratégia de DLP.
- ✓ Ao compreender os princípios e componentes básicos do DLP, sua estratégia de DLP levará ao estabelecimento de um programa bem-sucedido que fornecerá governança em torno da protecção de dados para a organização.

## Software antivírus (*Antivirus Software*):



## **Software antivírus (*Antivirus Software*):**

- ✓ O software antivírus é um tipo de software usado para prevenir, verificar, detectar e excluir vírus de um computador.
- ✓ Uma vez instalado, a maioria dos softwares antivírus serão executados automaticamente em segundo plano para fornecer protecção em tempo real contra ataques de vírus.
- ✓ Um número incalculável de novos vírus é descoberto diariamente, por isso é importante e crítico ter um software antivírus instalado e configurado para actualizar automaticamente para os arquivos de detecção mais recentes para ficar à frente das toneladas de códigos maliciosos que correm desenfreadamente na Internet.
- ✓ Os criadores de malware hoje são realmente conhecedores de como explorar pontos fracos em sistemas de computador.

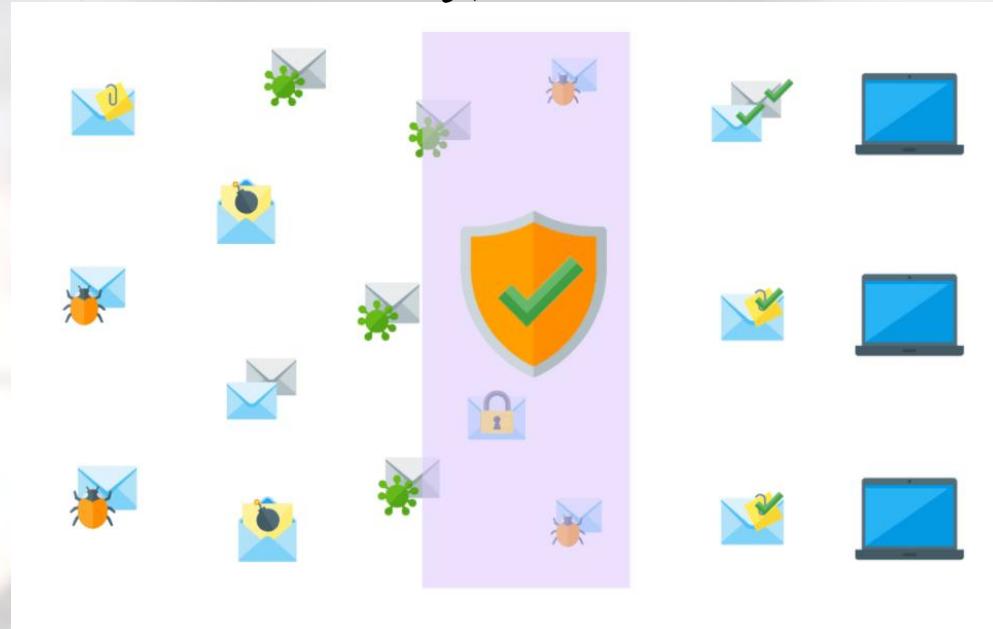
## Detecção e Resposta de *Endpoint* (*Endpoint Detection and Response -EDR*):



## **Detecção e Resposta de *Endpoint* (*Endpoint Detection and Response -EDR*):**

- ✓ O EDR fornece às equipes de segurança a visibilidade de que precisam para descobrir incidentes que, de outra forma, permaneceriam invisíveis.
- ✓ O EDR é importante porque fornece uma visão gráfica de como o invasor obteve acesso ao sistema e o que ele fez quando entrou.
- ✓ O EDR pode detectar atividades maliciosas em um endpoint como resultado de explorações de vulnerabilidades conhecidas como zero day, ameaças persistentes avançadas, ataques sem arquivos ou sem malware, que não deixam assinaturas e podem, portanto, evitar antivírus legados.

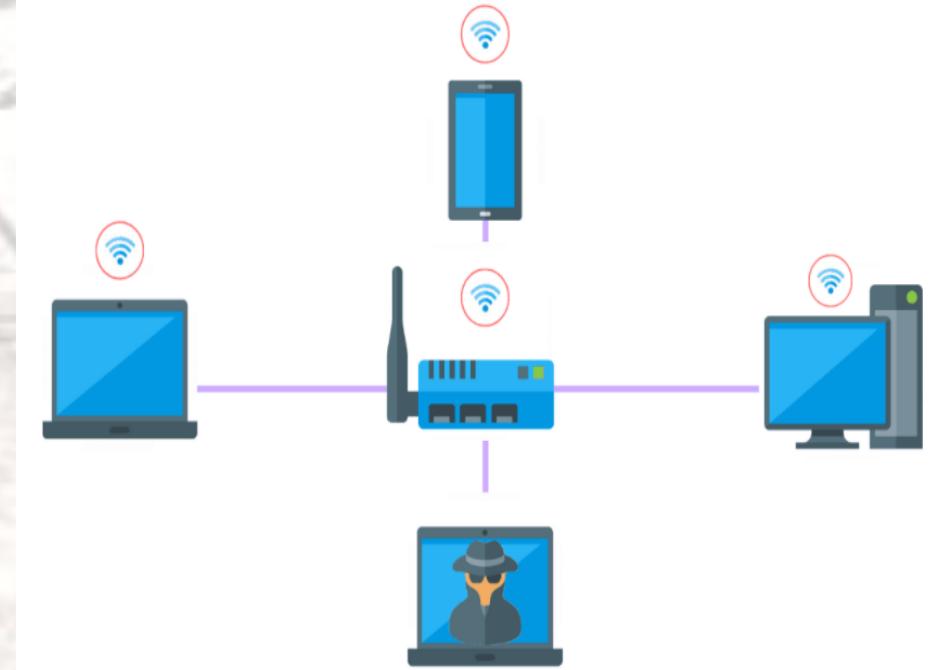
## Segurança de e-mail (*Email Security*):



- ✓ O e-mail é frequentemente usado para espalhar malware, spam e ataques de phishing.
- ✓ É importante que uma organização implemente a segurança de e-mail para proteger contra as várias formas de ataques cibernéticos por e-mail, bem como garantir que as mensagens confidenciais sejam criptografadas à medida que transitam da rede para o destinatário.

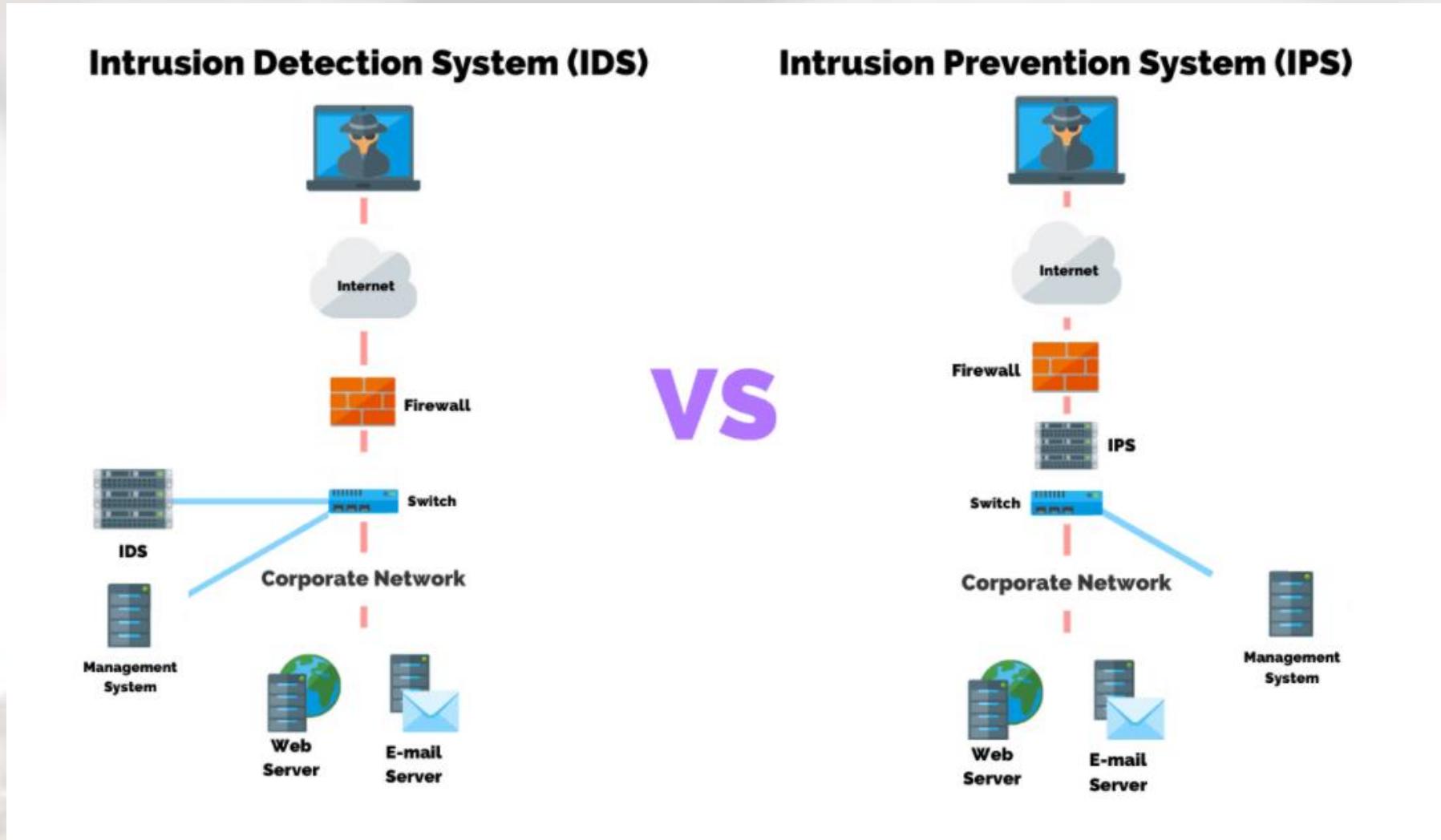
## Segurança em redes sem fio (*Wireless Security*):

- ✓ A segurança em redes sem fio é definida como a protecção de acesso não autorizado e tentativas maliciosas a uma rede sem fio ou Wi-Fi.
- ✓ Implementar uma forte segurança em redes sem fio é importante hoje, pois muitas organizações permitem que seus funcionários trabalhem remotamente e se conectem à Internet por meio de uma rede sem fio.
- ✓ O WiFi é altamente susceptível a hackers se protocolos sem fio fracos estiverem activados. Uma rede sem fio projectada com os protocolos de segurança sem fio actuais, como o WPA2, pode impedir ataques cibernéticos.



# Fundamentos de SR

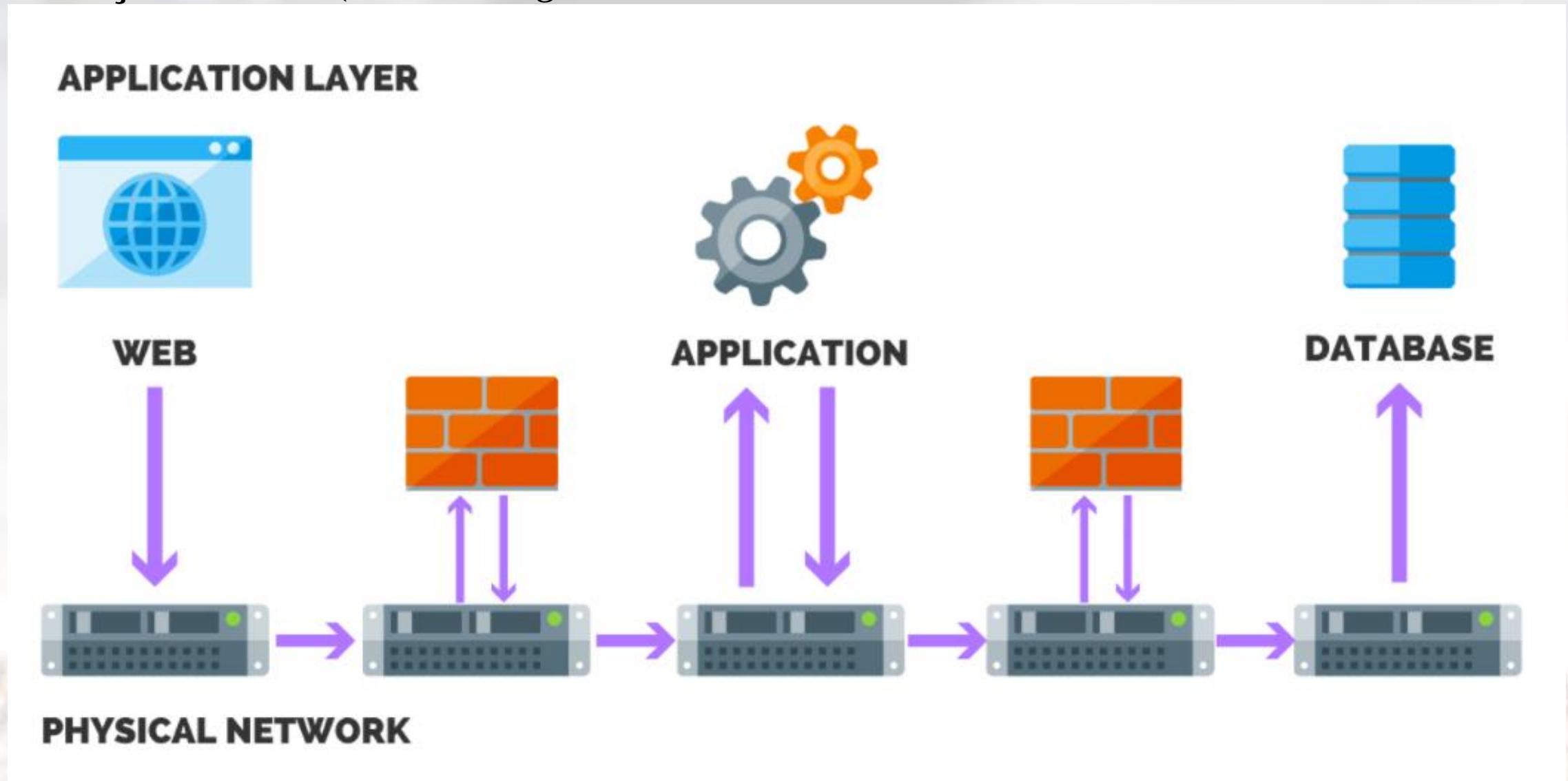
IDS/IPS:



## **IDS/IPS:**

- ✓ IPS/IDS são medidas de segurança de rede que são implantadas em uma rede para detectar e interromper possíveis incidentes. Os termos geralmente estão vinculados, mas são distintos em termos de funcionalidade.
- ✓ A principal diferença entre um sistema de detecção de intrusão (IDS) e um sistema de prevenção de intrusão (IPS) é que um IDS é usado para monitorar uma rede, que envia alertas quando são detectados eventos suspeitos em um sistema ou rede. Enquanto que, um IPS reage a ataques em andamento com o objectivo de impedir que eles alcancem sistemas e redes alvo.
- ✓ IPS/IDS são peças críticas para a infraestrutura de segurança de uma organização porque um dispositivo pode detectar e relatar um ataque enquanto o outro pode interromper ataques com base em políticas de segurança.
- ✓ Em equipamentos de rede modernos, é comum que ambas as tecnologias sejam combinadas em um único dispositivo Unified Threat Management.

## Segmentação de rede (*Network Segmentation*)

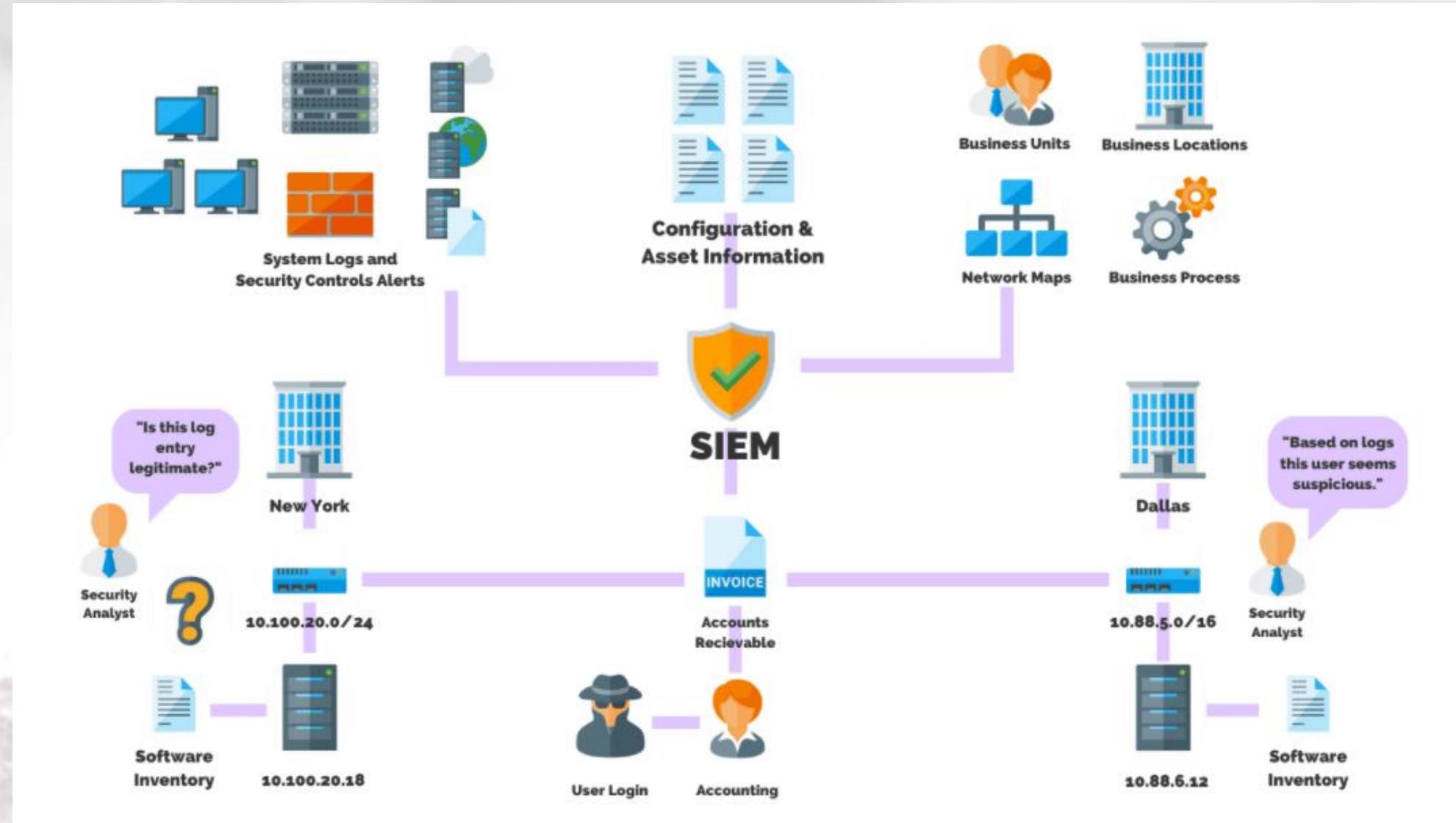


## **Segmentação de rede (*Network Segmentation*)**

- ✓ A segmentação de rede é uma abordagem arquitetônica que divide uma rede em vários segmentos ou micro sub-redes, cada uma actuando como sua própria pequena rede.
- ✓ Isso permite que os administradores de rede controlem o fluxo de tráfego entre sub-redes com base em políticas granulares.
- ✓ A segmentação de rede é importante porque permite que as organizações não apenas melhorem o monitoramento e o desempenho, mas, principalmente, aprimorem a segurança da rede.
- ✓ A segmentação de rede pode impedir a propagação de malware isolando uma rede em uma área, mantendo outro segmento da rede protegido.

# Fundamentos de SR

## SIEM (*Security Information and Event Management*)



## **SIEM (*Security Information and Event Management*)**

- ✓ Uma solução de Gestão de Informações e Eventos de Segurança (SIEM) oferece suporte à detecção de ameaças, conformidade e gestão de incidentes de segurança por meio da colecta e análise (tanto em tempo quase real quanto histórico) de eventos de segurança, bem como uma ampla variedade de outras fontes de dados contextuais e de eventos
- ✓ Um SIEM tem três características principais que o tornam importante para uma organização. Esses recursos incluem a detecção de incidentes para criar uma linha do tempo de ataque, gerir incidentes e é uma fonte de log que atende aos requisitos de conformidade e regulamentares.

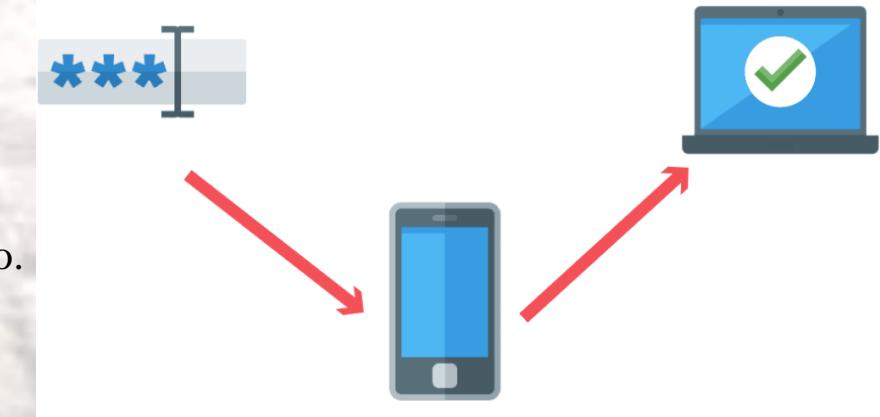
## Segurança da Web (*Web Security*)

- ✓ A segurança da Web é definida como a protecção de um aplicativo da Web que é exposto à Internet.
- ✓ O nível de protecção engloba ferramentas ou recursos que detectam, previnem e respondem a ameaças cibernéticas.
- ✓ Muitas organizações anunciam ao público seus serviços, fornecem um meio conveniente para aceitar pagamentos online e trocar informações pessoais.
- ✓ A segurança na Web é importante porque protege a identidade e a reputação de uma organização.
- ✓ As estratégias para impedir ataques e fortalecer a segurança da Web incluem técnicas de codificação seguras, garantindo que o site da Web suporte apenas os protocolos SSL/TLS actuais, verificação frequente de vulnerabilidades/aplicativos da Web e testes de penetração.



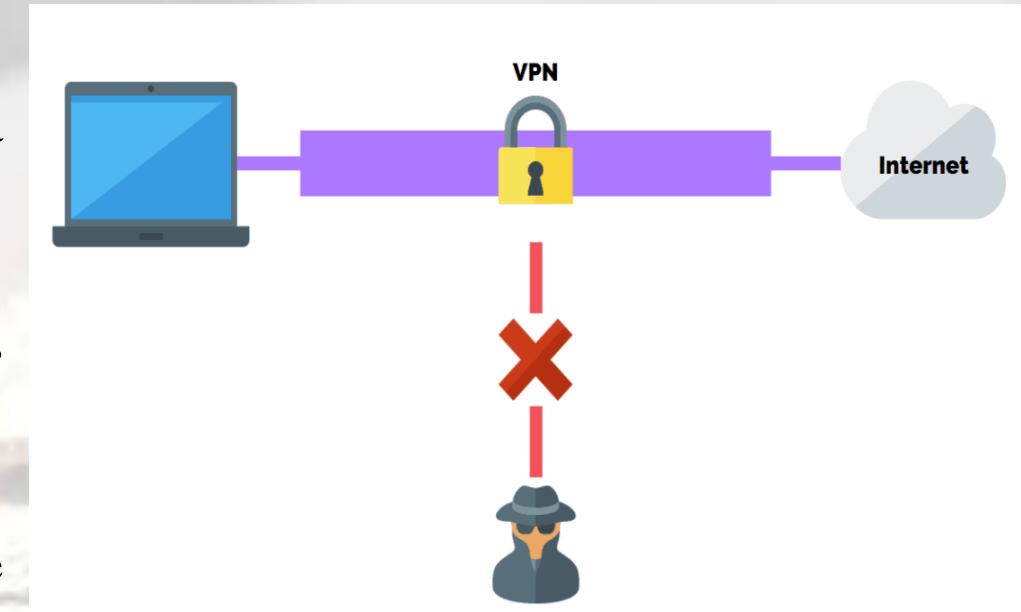
## Autenticação Multifator (*Multifactor Authentication -MFA*)

- ✓ A autenticação multifator, ou comumente chamada de MFA, é um sistema de autenticação que requer mais de um factor de autenticação distinto para uma autenticação bem-sucedida.
- ✓ A autenticação multifator pode ser realizada usando um autenticador multifator ou por uma combinação de autenticadores que fornecem diferentes factores.
- ✓ Os três factores de autenticação são algo que você conhece (SYK), algo que você tem (SYH) e algo que você é (SYA).
- ✓ A MFA é importante porque, se seu nome de utilizador e senha forem roubados por meio de uma violação de dados, o invasor cibernético não terá o factor de autenticação adicional para concluir a autenticação.
- ✓ Exemplos de factores de autenticação são:
  - Algo que você sabe – Senha/PIN.
  - Algo que você possui – Token de Hardware/Software emitido por sua organização.
  - Algo que você é – Biométrico (Impressão digital, IRIS/Retina Scan).



## Rede Privada Virtual (*Virtual Private Network -VPN*)

- ✓ Uma Rede Privada Virtual, ou VPN, é uma conexão criptografada pela Internet de um dispositivo para uma rede.
- ✓ A conexão criptografada ajuda a garantir que os dados confidenciais sejam transmitidos com segurança.
- ✓ Ela impede que pessoas não autorizadas escutem o tráfego e permite que o utilizador realize o trabalho remotamente.
- ✓ As VPNs são importantes para empresas e consumidores, pois uma organização pode incluir um pacote VPN padrão para que seus funcionários remotos se conectem à rede do escritório como se estivessem no escritório.
- ✓ A VPN fornece um túnel seguro entre o cliente VPN e o servidor VPN da organização, o que impede que o invasor cibernético veja informações confidenciais.



## Principais ameaças à segurança de rede em 2021

### Engenharia Social (*Social Engineering*)

- ✓ A engenharia social é uma técnica de manipulação que explora o erro humano para obter informações privadas, acesso ou valores.
- ✓ As formas comuns de engenharia social incluem:
  - **Phishing** – Refere-se a um ataque que geralmente é enviado na forma de um link embutido em um e-mail. A mensagem é disfarçada e parece um e-mail de uma fonte confiável, mas geralmente é um link para um site malicioso.
  - **Vishing** – Este ataque tenta induzir as vítimas a fornecer informações confidenciais por telefone. Na maioria dos casos, o invasor manipula estrategicamente as emoções humanas, como medo, simpatia e ganância para atingir seus objectivos.
  - **Smishing** – Um ataque cibernético que usa mensagens de texto SMS para enganar suas vítimas e fornecer informações confidenciais a um cibercriminoso.

## Principais ameaças à segurança de rede em 2021

### Vulnerabilidades não corrigidas (*Unpatched Vulnerabilities*)

- ✓ Vulnerabilidades não corrigidas referem-se a um programa ou código de software que contém uma falha.
- ✓ A falha ou bug no código geralmente é tornado público. Isso permite que um invasor cibernético execute seu código malicioso contra a falha conhecida.
- ✓ Uma vez bem-sucedido, o invasor rastreará e procurará sistemas vulneráveis, com o objectivo de explorar o sistema.
- ✓ Sistemas sem patches e pontos de acesso mal protegidos permitem que os agentes de ameaças comprometam muitas empresas.

## **Principais ameaças à segurança de rede em 2021**

### **Ransomware**

- ✓ Ransomware é um tipo de software malicioso projectado para bloquear o acesso a um sistema de computador até que uma quantia em dinheiro seja paga.
- ✓ A crescente pressão para se submeter à extorsão, o direcionamento das vítimas mais vulneráveis e as táticas que dificultam a recuperação de dados criptografados mantem o ransomware como a “linha de negócios” mais lucrativa para os cibercriminosos e a maior ameaça para todas as organizações.

### **Ameaças internas**

- ✓ Uma ameaça interna é definida como a ameaça de que um funcionário ou contratado usará seu acesso autorizado, intencionalmente ou não, para prejudicar a segurança de seu empregador.
- ✓ De acordo com o relatório de violação de dados da Verizon de 2020, os insiders foram responsáveis por uma violação de dados em 30% dos casos. Com os funcionários trabalhando em casa hoje devido à pandemia do COVID-19, os empregadores não podem ver fisicamente o que seus funcionários estão fazendo.

# Actividade



## **TRABALHO INDIVIDUAL 3:**

1. Leia e faça o resumo das secções abaixo indicadas do livro *Criptography and Network Security: principles and practice*, William Stallings, 6 Ed.
  - Secção 1.3 *Security attack*
  - Secção 1.4 *Security Services*
  - Secção 1.5 *Security Mechanisms*
2. Responda as questões de revisão (Review questions), constantes na página 25 do livro *Criptography and Network Security: principles and practice*, William Stallings, 6 Ed.

**Data de Entrega: 03/04/2023**

# Bibliografia



# Bibliografia

1. Segurança de redes / Angelo Eduardo Nunan, Frank Douglas Cruz de Farias, Marcos Fabiano P. Santiago – Manaus/AM UEA Edições, 2010
2. PEREIRA, Marcos. MARCELO, Antonio. A Arte de Hackear Pessoas. São Paulo: Brasport, 2005
3. MITNICK, Kevin D. SIMON, Willian L. A Arte de Enganar, Ataques de Hackers: controlando o fator humano na segurança da informação. São Paulo: Pearson Makron Books, 2003.
4. NORTHCUTT, Stephen. Como detectar invasão em rede, um guia para analistas. Rio de Janeiro: Ciência Moderna, 2000.
5. SÊMOLA, Marcos. Gestão da Segurança da Informação: uma visão executiva, Rio de Janeiro: Campus Elsevier, 2002.

